Sysax Multi Server User manual

Table of Contents

1

Introduction to Sysax Multi Server

1.1. Introduction to Sysax Multi Server

Sysax Multi Server is a Secure FTP server, SSH2 secure shell server, Telnet server, and HTTPS file server combined into a single Windows program. It's robust, secure, and high-speed software architecture makes it suitable for business and personal file transfer needs.

Supports multiple internet protocols

All file transfer protocols including FTP, FTPS, and SFTP are supported in addition to HTTP and HTTPS based file transfers. Telnet and Secure shell access are also supported.

Supports Multiple Authentication Methods

The server can authenticate connections using existing windows user accounts, LDAP Active Directory servers, external databases accessible using ODBC, or Sysax server specific user accounts. Additionally, access to specific connection protocols may be restricted for individual user accounts.

Supports remote web-based administration

The server can be remotely administered using any web browser. Server settings can be modified on the fly. Activities of connected users can be modified in real time.

Runs FTP scripts based on server events

The server can run FTP scripts that are trigged by events such as user login, file transfer completion, file rename, and delete operations. The server event type, user name, user IP address, and corresponding file names are made available inside the script. The FTP scripts are identical to that supported by Sysax FTP Automation and can be used to send email, initiate file transfers, process local files, or run other programs.

Runs as a Windows service

The program runs as a Windows service and can be configured to automatically start on system boot up even when no user is logged on.

Free personal edition

A free personal edition that supports one connection at a time and unlimited account creation is available for non-commercial use.

Simple to set up and use

Sysax Multi Server is simple to set up and use on any Windows-based computer.

Supports both anonymous and account-based access

Sysax Multi Server enables you to set up both anonymous and password protected user accounts on the same computer.

High speed software architecture

The software architecture for Sysax Multi Server has been fine-tuned to support very high data transfer rates, and large volumes of user connections.

Protection against security breaches

Sysax Multi Server has been designed to safeguard against many types of malicious hacking attacks against the server.

Unlimited free customer support

Licensed users of Sysax Multi Server are eligible for unlimited free customer service.

2

Minimum System Requirements

2.1. System Requirements

Sysax Multi Server is compatible with Windows 7, Windows 2008, certified for Windows Vista and runs on all versions of the Microsoft Windows operating system including:

- Windows 95
- Windows 98
- Windows 2000
- Windows ME
- Windows XP
- Windows 2003
- Windows Vista
- Windows 2008
- Windows 7

The minimum hardware required to run Sysax Multi Server are:

- Pentium Class or higher processor
- At least 16MB of free system RAM
- At least 10MB of hard disk space
- Connection to the internet or local network

Note

Sysax Multi Server supports a multi-threaded architecture that scales well on multi-core and multi-processor systems.

3

How to Install/Uninstall

3.1. Install/Uninstall Sysax Multi Server

To install Sysax Multi Server:

1. Verify that the downloaded msi installation package is digitally signed by Codeorigin, LLC
2. Double click on the msi installation package to run the installation wizard
3. Follow on-screen instructions to install Sysax Multi Server

To uninstall Sysax Multi Server:

1. Click the **Start** button on your computer
2. Select the **All Programs** Menu
3. Select **Sysax Multi Server**
4. Click on **Uninstall Sysax Multi Server**
5. Follow on-screen instructions to **uninstall** Sysax Multi Server

or

1. Click the **Start** button
2. Select **Settings**
3. Select **Control Panel**
4. Select **Add/Remove Programs**
5. Choose **Sysax Multi Server** from the list
6. Click **Add/Remove** button
7. Follow on-screen instructions to uninstall Sysax Multi Server

4

Selecting and Installing a License

4.1. Selecting and Installing a License

The Sysax Multi Server installation package contains a 30-day trial license for the product. After the trial has expired, you will need to choose one of the following product editions. Visit **http://www.sysax.com/** to purchase a product license. Detailed comparison of all product editions is available at **http://www.sysax.com/server/compare.htm**

Enterprise Edition

Licensed for commercial use and simultaneously supports all of the following connection protocols: FTP, SFTP, FTPS, Telnet, SSH2 Secure Shell, HTTP and HTTPS. Unlimited users can also simultaneously connect to the server.

Professional Edition

Licensed for commercial use and supports any one of the following connection protocols: FTP, FTPS, SFTP, FTPS, Telnet, SSH2 Secure Shell, HTTTP and HTTPS. Up to 10 users can simultaneously connect to the server for HTTP and HTTPS file tranansfers. Unlimited users can connect using FTP, SFTP, FTPS, Telnet, and SSH2 Secure Shell.

Standard Edition

Licensed for commercial use and supports any one of the following connection protocols: FTP, FTPS, SFTP, FTPS, Telnet, and SSH2 Secure Shell. Up to 10 users can simultaneously connect to the server.

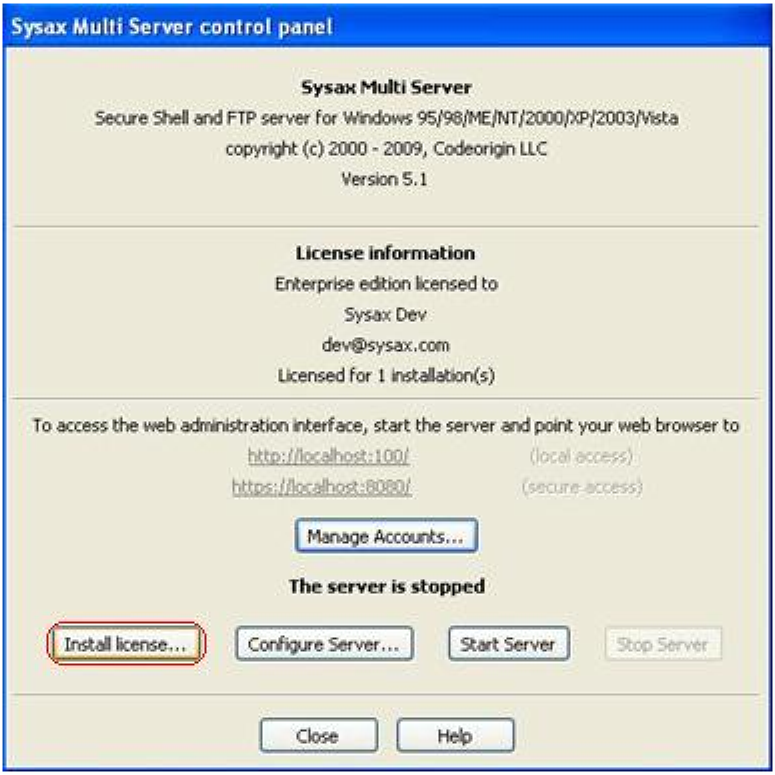
Personal edition (also known as the Free Edition)

Licensed only for personal use and supports any one of the following connection protocols: FTP, FTPS, SFTP, FTPS, Telnet, and SSH2 Secure Shell. One user can simultaneously connect to the server at a time.

To install a license:

1. Open the Sysax Multi Server Administration panel and click the **Install License** button (Figure 4.1).

Figure 4.1. Start License Installation



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

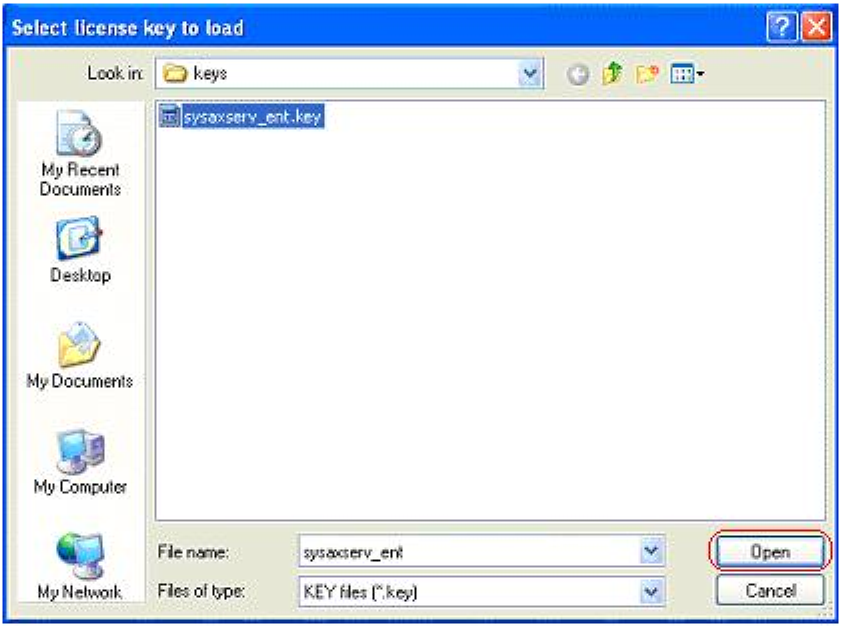
http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is stopped

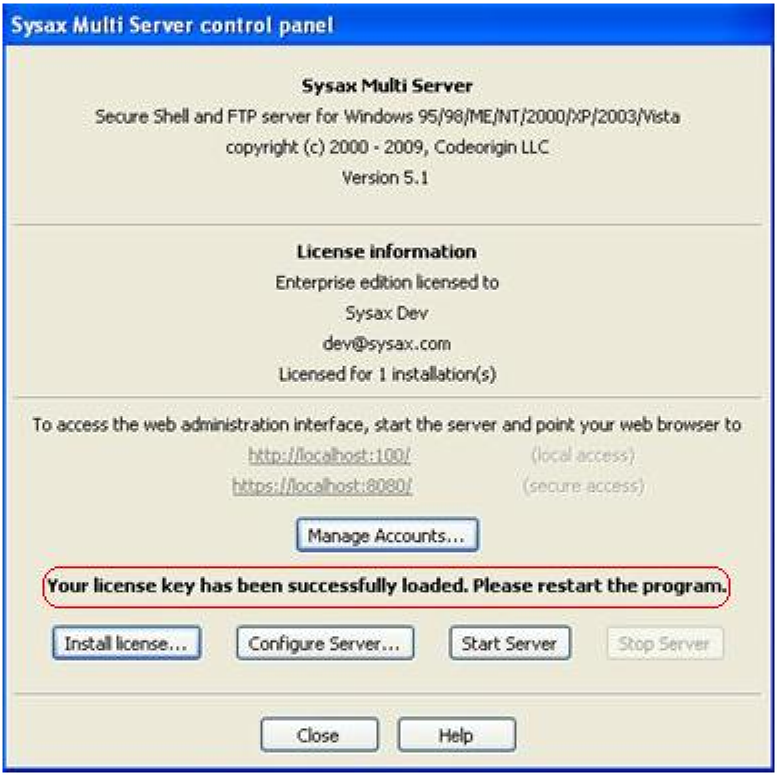
2. Select the License Key file and click the **Open** button (Figure 4.2).

Figure 4.2. Select License Key



3. Restart Sysax Multi Server to complete installation of the license(Figure 4.3).

Figure 4.3. Install License Key



Sysax Multi Server control panel

Sysax Multi Server
Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista
copyright (c) 2000 - 2009, Codeorigin LLC
Version 5.1

License information
Enterprise edition licensed to
Sysax Dev
dev@sysax.com
Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to
http://localhost:100/ (local access)
https://localhost:8080/ (secure access)

Your license key has been successfully loaded. Please restart the program.

License installation on Windows 7, 2008, and Vista

On Windows 7, Windows server 2008, and Windows Vista, you may need to manually install the license key as follows:

Open a DOS prompt and navigate to the folder where you have saved the license key file (eg. sysaxserv_ent.key) and run the following command:

```
sysaxservdmgr.exe /installlic sysaxserv_ent.key
```

You should see the new license information when you close and reopen the Sysax Multi Server Administrator panel.

The sysaxservdmgr.exe program is located in the installation folder for Sysax Multi Server. If your system cannot automatically find it, you may need to type in the full path to the executable or copy the license file to the installation folder, navigate to this folder from the DOS command prompt, and run the command.

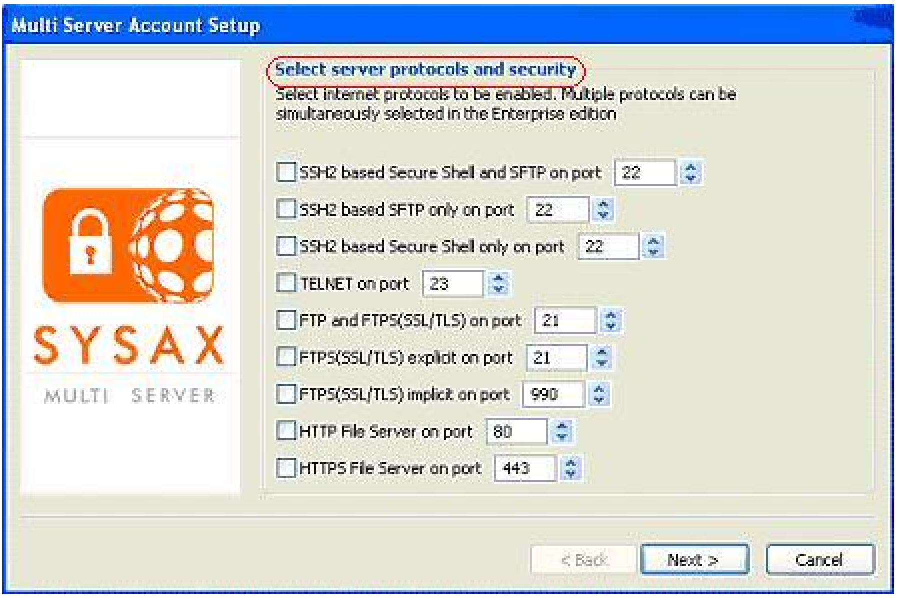
5

Settings for Sysax Multi Server Control Panel

5.1. Setting-up Connection protocols

Sysax Multi Server supports secure file transfer protocols such as FTPS, SFTP, and HTTPS in addition to SSH2 Secure Shell. FTP, HTTP, and Telnet are also supported. The **Enterprise Edition** allows multiple protocols to be simultaneously selected. The **Professional and Personal Editions** allows the selection of a single protocol at a time. If multiple protocols are simultaneously enabled, each protocol must have a different port number associated with it.

Figure 5.1. Multi Server Account Setup



Multi Server Account Setup

Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

- □ SSH2 based Secure Shell and SFTP on port 22
- □ SSH2 based SFTP only on port 22
- □ SSH2 based Secure Shell only on port 22
- □ TELNET on port 23
- □ FTP and FTPS(SSL/TLS) on port 21
- □ FTPS(SSL/TLS) explicit on port 21
- □ FTPS(SSL/TLS) implicit on port 990
- □ HTTP File Server on port 80
- □ HTTPS File Server on port 443

- **SSH2 based Secure Shell and SFTP**

  This option enables Secure shell so that users can remotely login and have access to a command prompt. It also enables file transfer using SFTP. In both cases, data transfer is protected with SSH2 based encryption. The default connection port number is 22.

- **SSH2 based SFTP only**

  This option only enables file transfer using SFTP. Secure Shell access is disabled and users will not have access to a command prompt. In this case, data transfer is protected with SSH2 based encryption. The default connection port number is 22.

- **SSH2 based Secure Shell only**

This option only enables remote login access without the ability to transfer files. Connected users have access to a command prompt to run commands on the system. The connection is protected with SSH2 based encryption. The default connection port number is 22.

- **Telnet**

  This option enables unsecured remote login access without the ability to transfer files. Connected users have access to a command prompt to run commands on the system. The connection is not encrypted and can be used within internal networks to eliminate the additional overhead associated with encryption. The default connection port number is 23.

- **FTP and FTPS(SSL/TLS)**

  This option enables unsecured file transfer using FTP or secured file transfer using SFTP. FTP connections are not encrypted and can be used within internal networks to eliminate additional overhead associated with encryption. FTPS connections are protected with SSH/TLS based encryption. The default connection port number in both cases is **21**.

- **FTPS(SSL/TLS) Explicit**

  This option only enables file transfer using explicit FTPS. In explicit FTPS, the connection is first established without encryption. An encryption mechanism based on SSL/TLS is then negotiated and subsequent data transfers are encrypted. The default connection port is 21.

- **FTPS(SSL/TLS) Implicit**

  This option only enables file transfer using implicit FTPS. In implicit FTPS, the connection is always encrypted with SSL/TLS. The default connection port is 990.

- **HTTP File Server**

  This option enables files to be transferred using a regular web browser such as Internet Explorer. The connection is not encrypted and can be used within internal networks, eliminating the additional overhead associated with encryption. The default connection port is 80.

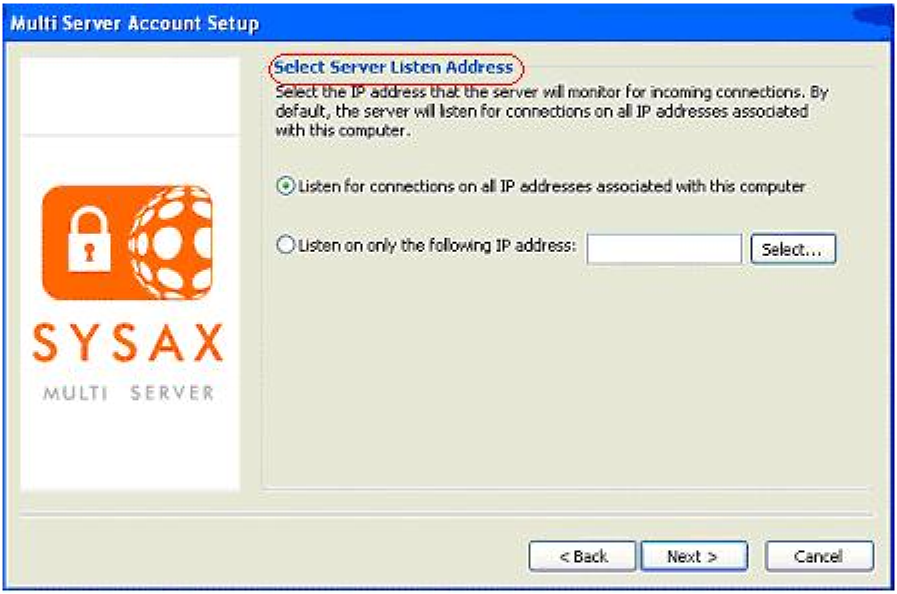
- **HTTPS File Server**

  This option enables files to be securely transferred using a regular web browser such as Internet Explorer. The connection is protected with SSL/TLS based encryption.

5.2. Selecting Server Listen Address

After setting up the connection protocols, the next step is to select the IP address that the server will monitor for incoming connections. There are two options are available in this section. By default, the server will listen for connections on all addresses associated with this computer. This default radio button is pre-selected.

Figure 5.2. Select Server Listen Address



Multi Server Account Setup

Select Server Listen Address

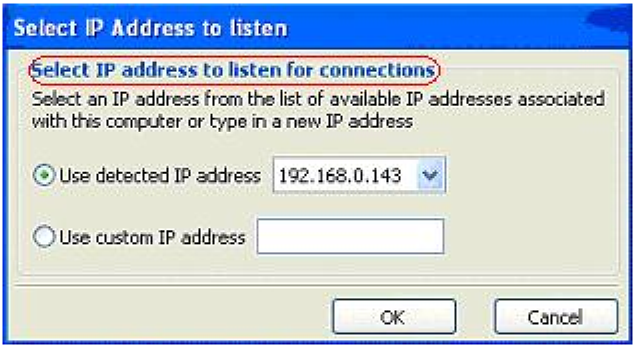
Select the IP address that the server will monitor for incoming connections. By default, the server will listen for connections on all IP addresses associated with this computer.

● Listen for connections on all IP addresses associated with this computer

○ Listen on only the following IP address:

To make the server listen only for connections on a specific IP address, select the **Listen on only the following IP address** radio button. Click on the **Select** button to select an IP address from the list of available IP addresses associated with the computer or type in a new IP address.

Figure 5.3. Select IP Address to Listen



Select IP Address to listen

Select IP address to listen for connections

Select an IP address from the list of available IP addresses associated with this computer or type in a new IP address

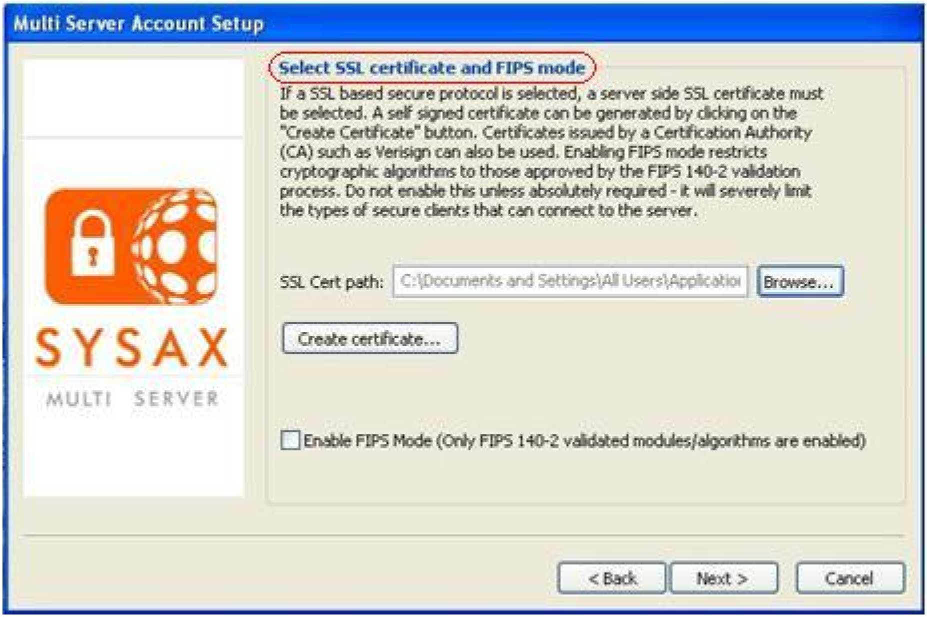
● Use detected IP address 192.168.0.143

○ Use custom IP address

5.3. Installing SSL Certificate

A self signed SSL certificate is automatically created on product installation. A different SSL certificate may be selected by clicking on the **Browse** button. SSL Certificates are required if FTPS or HTTPS protocols are used for file transfer. (Note: Enabling FIPS Mode will restrict the cryptographic algorithms used to those approved by the FIPS 140-2 validation process.)

Figure 5.4. Select SSL Certificate



Multi Server Account Setup

Select SSL certificate and FIPS mode

If a SSL based secure protocol is selected, a server side SSL certificate must be selected. A self signed certificate can be generated by clicking on the "Create Certificate" button. Certificates issued by a Certification Authority (CA) such as Verisign can also be used. Enabling FIPS mode restricts cryptographic algorithms to those approved by the FIPS 140-2 validation process. Do not enable this unless absolutely required - it will severely limit the types of secure clients that can connect to the server.

SSL Cert path: C:\Documents and Settings\All Users\Applicatio

☐ Enable FIPS Mode (Only FIPS 140-2 validated modules/algorithms are enabled)

A new self signed certificate can also be created by clicking on the **Create Certificate** button. The certificate generation dialog box is displayed. The SSL certificate parameters to be filled out are:

Server Name

This field specifies the domain name of the server.

Group Name

This field specifies the group or division name of the company or organization that the server belongs to.

Company Name

This field specifies the name of the company or organization that the server belongs to.

City Name

This field specifies the name of the city that the company or organization is located in.

State Name

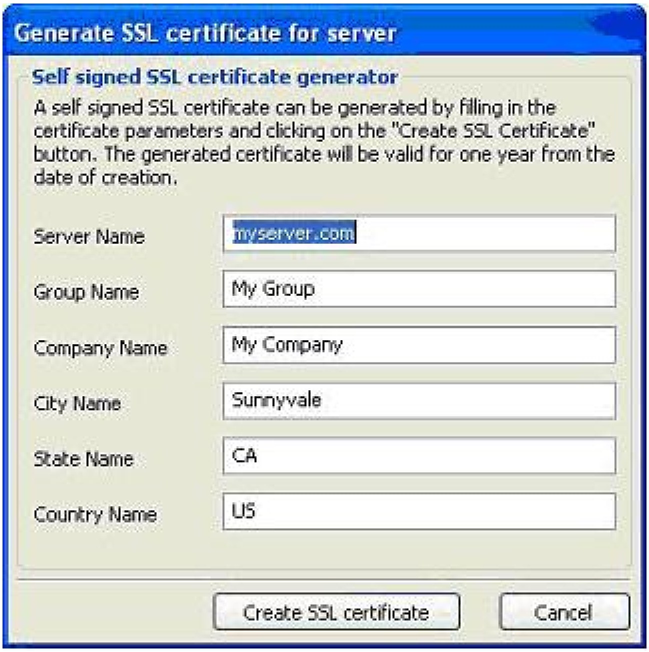
This field specifies the name of the state that the company or organization is located in.

Country Name

This field specifies the two letter country code that the company or organization is located in.

The new SSL certificate is then generated by clicking the **Create SSL Certificate** button.

Figure 5.5. Generate SSL Certificate



Generate SSL certificate for server

Self signed SSL certificate generator

A self signed SSL certificate can be generated by filling in the certificate parameters and clicking on the "Create SSL Certificate" button. The generated certificate will be valid for one year from the date of creation.

Server Name: myserver.com

Group Name: My Group

Company Name: My Company

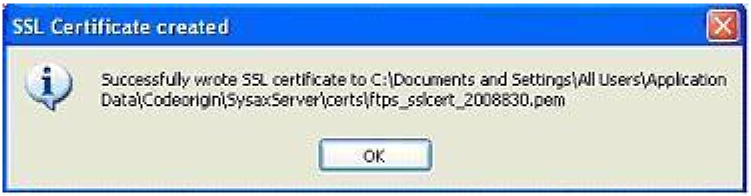
City Name: Sunnyvale

State Name: CA

Country Name: US

Click **OK** on the SSL Certificate created screen.

Figure 5.6. SSL Certificate Created



SSL Certificate created

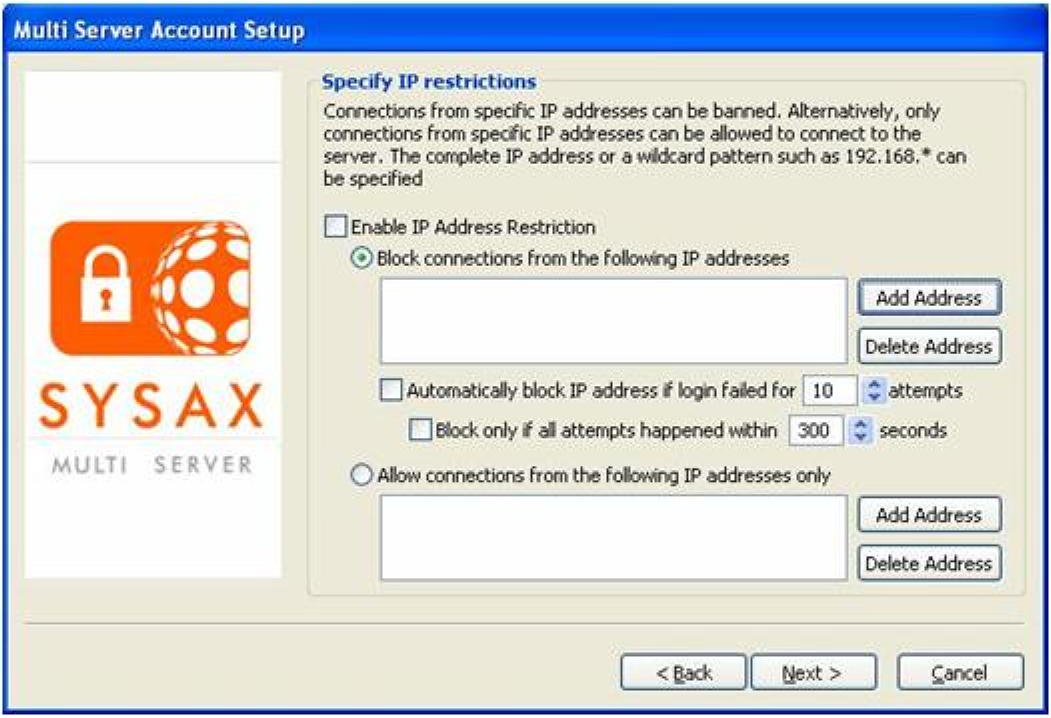
Successfully wrote SSL certificate to C:\Documents and Settings\All Users\Application Data\Codeorigin\SysaxServer\certs\ftps_sslcert_2008830.pem

The generated server-side self-signed SSL certificate is valid for one year from the date of creation.

5.4. Restricting IP addresses

Connections to Sysax Multi Server can be controlled by banning specific IP addresses or by allowing only specific IP addresses. The complete IP address of the connection or a combination of IP addresses and wildcards such as 192.168.* can be specified.

Figure 5.7. Specify IP Restrictions



Multi Server Account Setup

Specify IP restrictions

Connections from specific IP addresses can be banned. Alternatively, only connections from specific IP addresses can be allowed to connect to the server. The complete IP address or a wildcard pattern such as 192.168.* can be specified

□ Enable IP Address Restriction

● Block connections from the following IP addresses

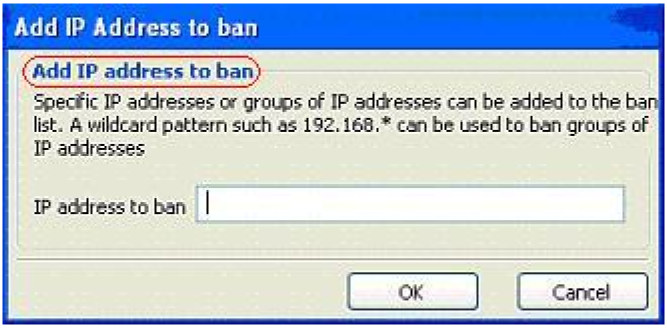
□ Automatically block IP address if login failed for 10 attempts

□ Block only if all attempts happened within 300 seconds

○ Allow connections from the following IP addresses only

To ban IP addresses, click the radio button **Enable IP Address Restriction** and select the **Block Connections** option. Choose whether to **automatically block IP address if login failed** or whether to **block only if attempts happened within a certain number of seconds**. Click on the **Add Address** button to add IP addresses that need to be blocked.

Figure 5.8. Add IP Address to Ban



Add IP Address to ban

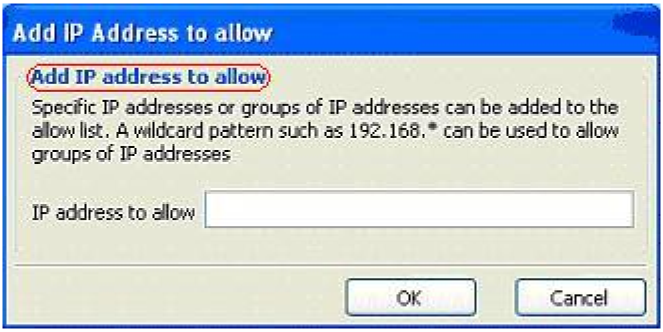
Add IP address to ban

Specific IP addresses or groups of IP addresses can be added to the ban list. A wildcard pattern such as 192.168.* can be used to ban groups of IP addresses

IP address to ban

To allow only specific IP addresses, select the **Allow connections** radio box (Figure 5.7). Click on the **Add Address** button to add IP addresses that need to be allowed.

Figure 5.9. Add IP Address to Allow



Add IP Address to allow

Add IP address to allow

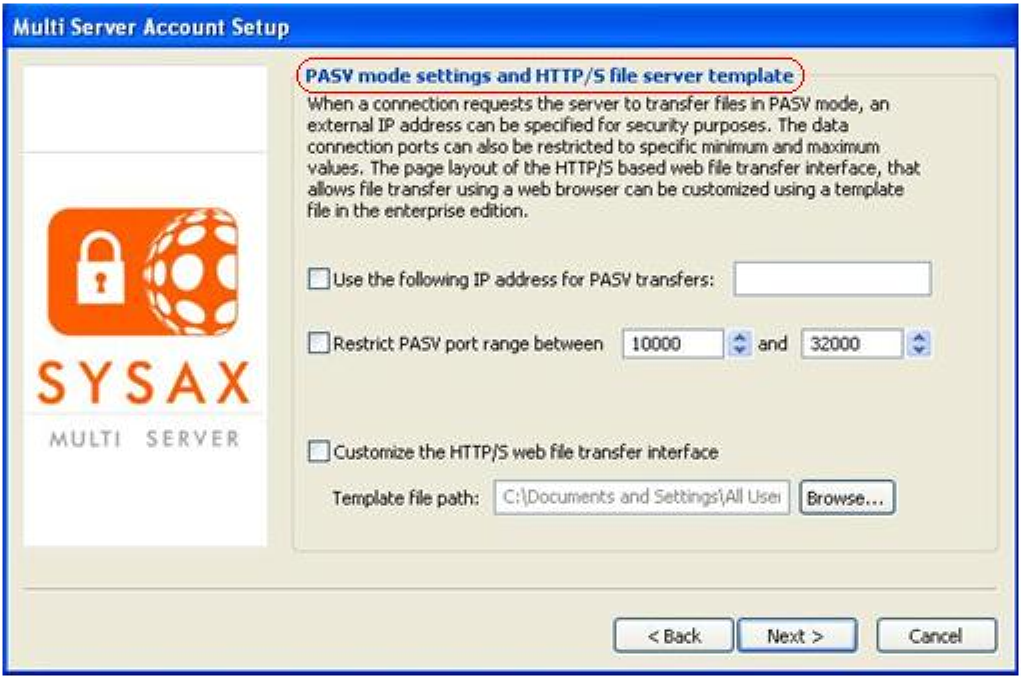
Specific IP addresses or groups of IP addresses can be added to the allow list. A wildcard pattern such as 192.168.* can be used to allow groups of IP addresses

IP address to allow

5.5. Restricting PASV Mode Settings and HTTP/S File Server Template

When a connection requests the server to transfer files in PASV mode, an external IP address can be specified for security purposes. If the Server is running inside a firewall or other secured environment, an IP address that is externally accessible is required. The range of data connection ports can also be restricted to specific minimum and maximum values.

Figure 5.10. Restrict PASV Mode Settings and HTTP/S File Server Template



PASV mode settings and HTTP/S file server template

When a connection requests the server to transfer files in PASV mode, an external IP address can be specified for security purposes. The data connection ports can also be restricted to specific minimum and maximum values. The page layout of the HTTP/S based web file transfer interface, that allows file transfer using a web browser can be customized using a template file in the enterprise edition.

□ Use the following IP address for PASV transfers:

□ Restrict PASV port range between 10000 and 32000

□ Customize the HTTP/S web file transfer interface

Template file path: C:\Documents and Settings\All User

The page layout of the HTTP/S based web file transfer interface that allows file transfer using a web browser can be customized using a template file in the enterprise edition (Figure 5.10). Click **Browse** button to quickly identify and select the template file path. The default template file is web-ft-template.txt. If the template is enabled, the file transfer interface can be changed by changing the template. The template can be customized as needed or a new template file can be created.

The default **template file** looks like this:

Exhibit 5.1. Default Template File

```
[LOGINPAGETITLE]
Title: Sysax Multi Server Web File Access Server

[LOGINPAGEHEADER]
<hr>
<h3>Header: Login Page</h3>
<hr>

[LOGINPAGEIMAGETAG]
<img src="loginacc.gif" width="148" height="295" border=1>

[LOGINPAGEINFOTEXT]
InfoText: Sysax Multi Server Web File Access Server

[LOGINPAGEFOOTER]
<hr>
<center><small>Footer: Login Page</small></center>

[FILEPAGETITLE]
Title: Sysax Multi Server Web File Access Server

[FILEPAGEHEADER]
<hr>
<h3>Header: File Page</h3>
<hr>

[FILEPAGEFOOTER]
<hr>
<center><small>Footer: File Page</small></center>
```

[LOGINPAGETITLE] : This section is used to change the title of the login page.

[LOGINPAGEHEADER] : This section is used to add some header html code to the login page.

[LOGINPAGEIMAGETAG] : This section is used to control the display of the image on the login screen. The image file name should be the same because files that can be sent before logging in is restricted to protect against hackers.

[LOGINPAGEINFOTEXT] : This section is used to control the display of the informational text shown at the right of the image and above the login button.

[LOGINPAGEFOOTER] : This section is used to add some footer html code to the login page.

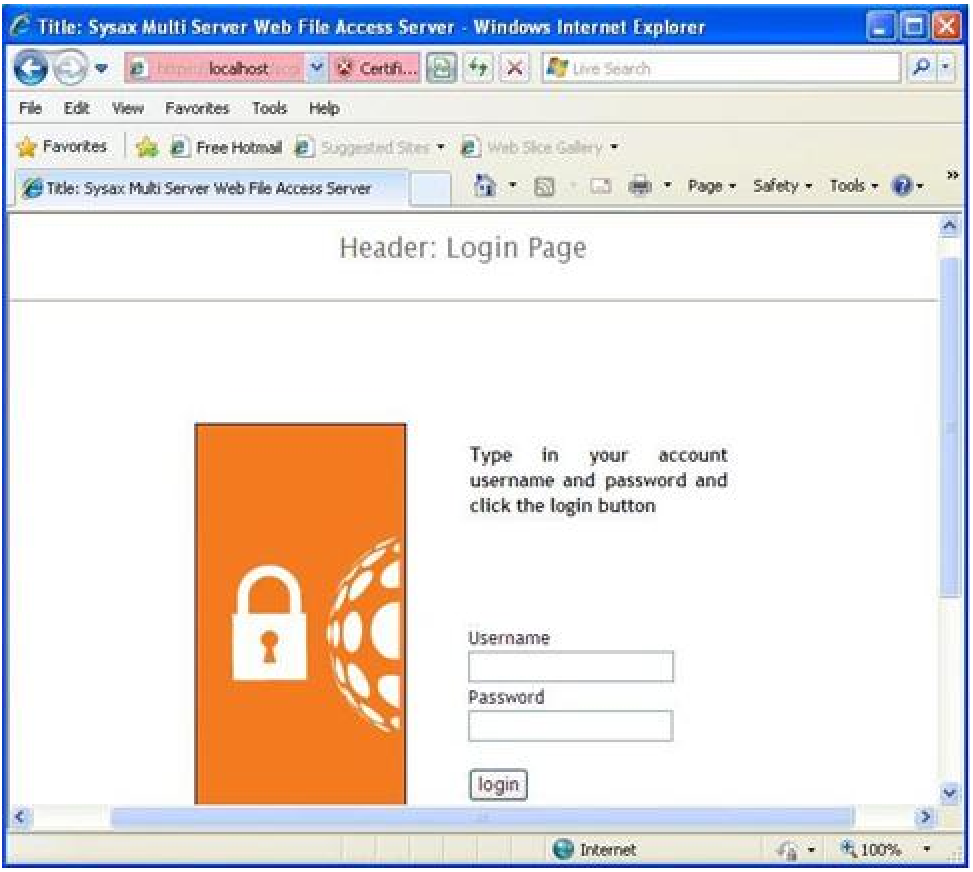
[FILEPAGETITLE] : This section is used to change the title of the file access pages.

[FILEPAGEHEADER] : This section is used to add some header html code to the file access pages.

[FILEPAGEFOOTER] : This section is used to add some footer html code to the file access pages.

When the default template is enabled, The login page of the HTTP/S File Transfer Interface appears as follows:

Figure 5.11. Login page of HTTPS File Transfer Interface



Header: Login Page

Type in your account username and password and click the login button

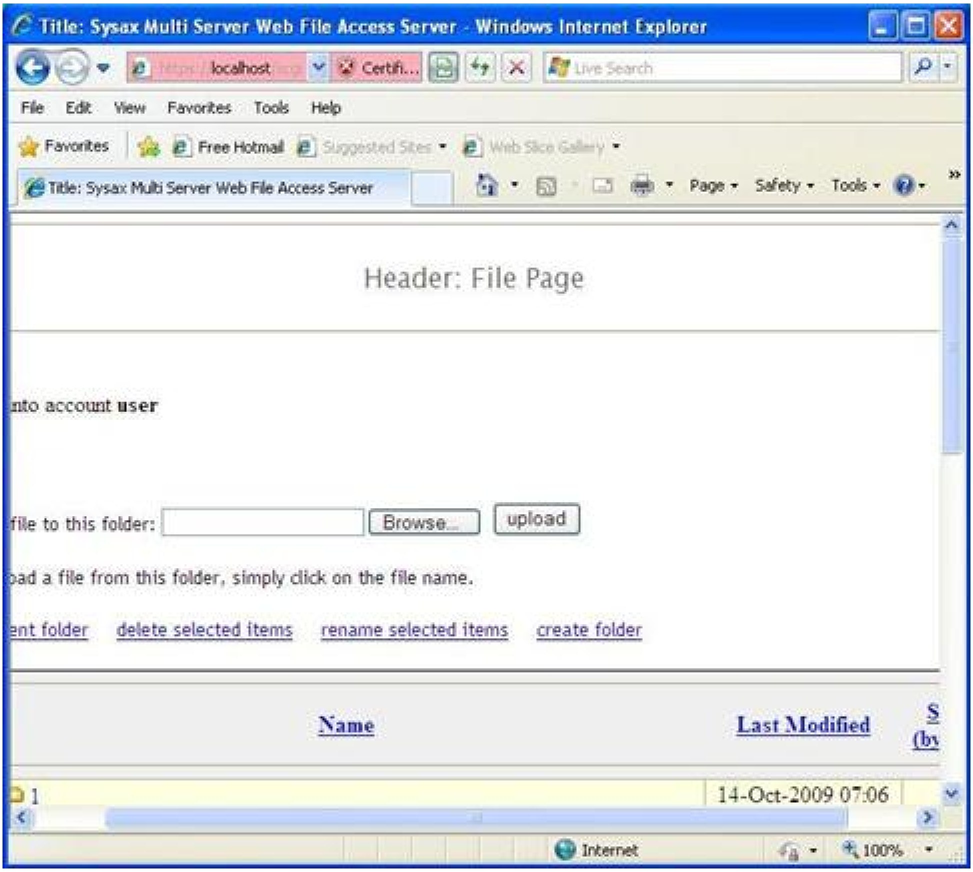
Username

Password

login

When the default template is enabled, The main page of the HTTP/S File Transfer Interface appears as follows:

Figure 5.12. HTTPS file transfer interface



Header: File Page

nto account **user**

file to this folder:

oad a file from this folder, simply click on the file name.

ent folder   delete selected items   rename selected items   create folder

Name	Last Modified	S (by
1	14-Oct-2009 07:06	

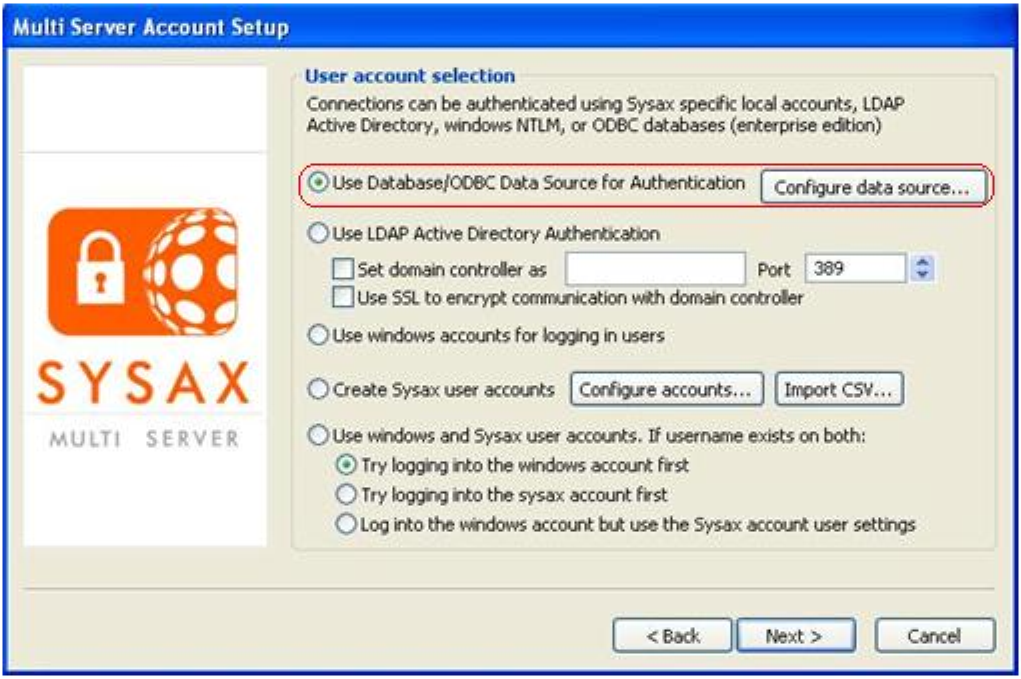
5.6. Setting-up User Accounts

User connections can be authenticated using ODBC databases (database authentication is supported in the enterprise edition), Windows NTLM, LDAP Active Directory, or Sysax Server specific local accounts

5.6.1. Authenticating using an ODBC Data Source

Sysax server can use an external ODBC Data Source to authenticate users

Figure 5.13. Authenticating with ODBC Data Source



User account selection

Connections can be authenticated using Sysax specific local accounts, LDAP Active Directory, windows NTLM, or ODBC databases (enterprise edition)

● Use Database/ODBC Data Source for Authentication

○ Use LDAP Active Directory Authentication

□ Set domain controller as Port 389

□ Use SSL to encrypt communication with domain controller

○ Use windows accounts for logging in users

○ Create Sysax user accounts

○ Use windows and Sysax user accounts. If username exists on both:

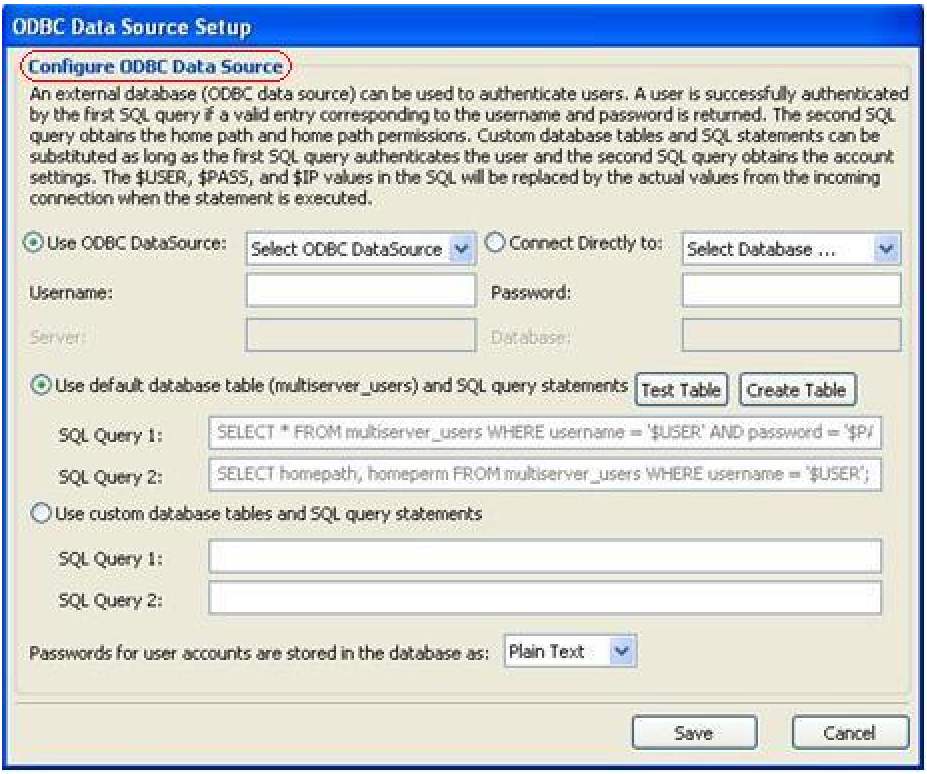
● Try logging into the windows account first

○ Try logging into the sysax account first

○ Log into the windows account but use the Sysax account user settings

Clicking on the **Configure data source** button opens the **ODBC Data Source Setup window**. In this, an external database(ODBC data source) can be used to authenticate users. A user is successfully authenticated by the first SQL query if a valid entry corresponding to the username and password is returned. The second SQL query obtains the home path and home path permissions. Custom database tables and SQL statements can be substituted as long as the first SQL query authenticates the user and the second SQL query obtains the account settings. The $USER, $PASS, and $IP values in the SQL will be replaced by the actual values from the incoming connection when the statement is executed.

Figure 5.14. Configure ODBC Data Source



ODBC Data Source Setup

Configure ODBC Data Source

An external database (ODBC data source) can be used to authenticate users. A user is successfully authenticated by the first SQL query if a valid entry corresponding to the username and password is returned. The second SQL query obtains the home path and home path permissions. Custom database tables and SQL statements can be substituted as long as the first SQL query authenticates the user and the second SQL query obtains the account settings. The $USER, $PASS, and $IP values in the SQL will be replaced by the actual values from the incoming connection when the statement is executed.

● Use ODBC DataSource: Select ODBC DataSource ○ Connect Directly to: Select Database ...

Username: Password:

Server: Database:

● Use default database table (multiserver_users) and SQL query statements

SQL Query 1: SELECT * FROM multiserver_users WHERE username = '$USER' AND password = '$P/

SQL Query 2: SELECT homepath, homeperm FROM multiserver_users WHERE username = '$USER';

○ Use custom database tables and SQL query statements

SQL Query 1:

SQL Query 2:

Passwords for user accounts are stored in the database as: Plain Text

The MS SQL Server Driver or MS Access Driver database option can be selected to connect directly to these Microsoft databases.

An example of the ODBC tables is shown below. The SQL statement that is executed to create the tables is similar to:

```
CREATE TABLE multiserver_users (uid INTEGER PRIMARY KEY NOT NULL, username
 VARCHAR (255) UNIQUE NOT NULL, password VARCHAR (255) NULL, homepath
 VARCHAR (255) NULL, homeperm VARCHAR (255) NULL, accdisabled INTEGER
 NULL);
```

In this:

- The username field is the username for the account and must be unique.
- The password field is the password for the account.
- The homepath field is the home path for the account.

- The homeperm field shows the permissions for the home path and all sub folders.

For the permissions field, the following letters mean:

R = file read

W = file write

D = file delete

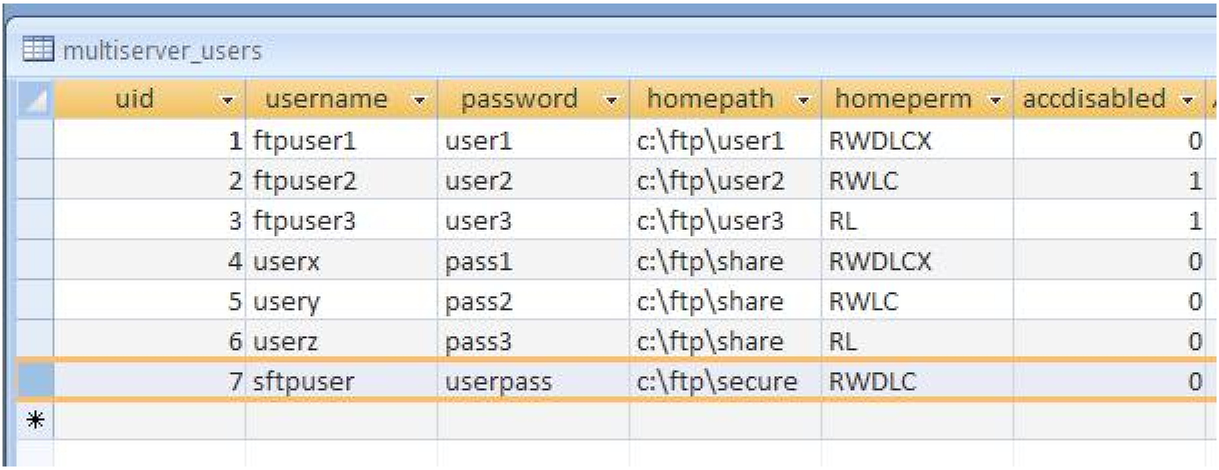
L = folder list

C = folder creates

X = folder delete

The accdisabled field shows if the account is disabled. An account is disabled if this field is set to 1.

Figure 5.15. ODBC Table



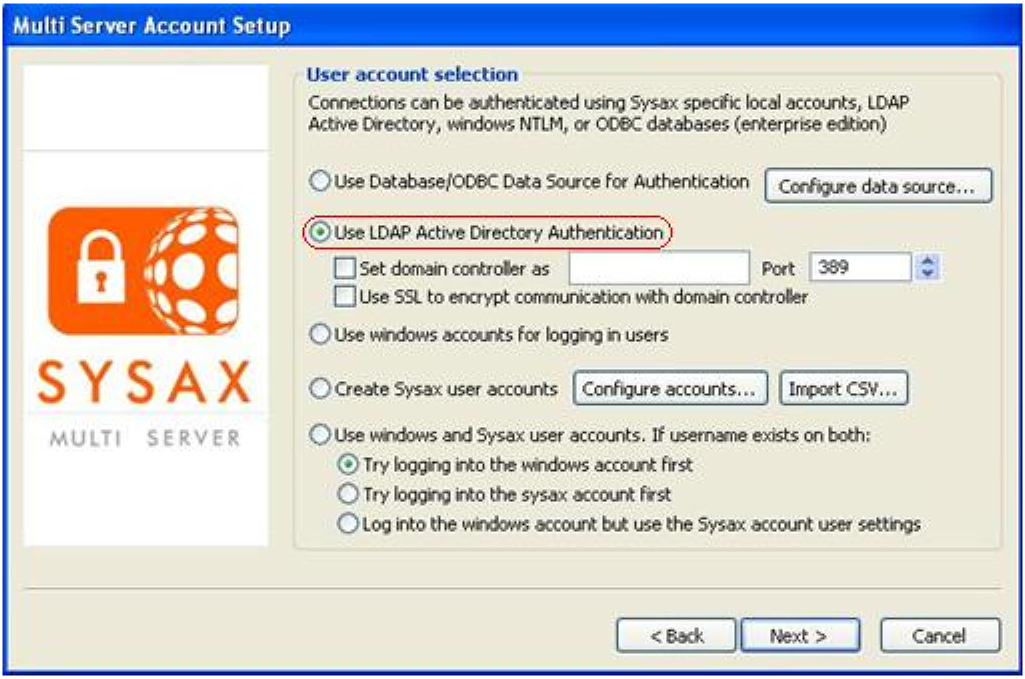
multiserver_users

uid	username	password	homepath	homeperm	accdisabled
1	ftpuser1	user1	c:\ftp\user1	RWDLCX	0
2	ftpuser2	user2	c:\ftp\user2	RWLC	1
3	ftpuser3	user3	c:\ftp\user3	RL	1
4	userx	pass1	c:\ftp\share	RWDLCX	0
5	usery	pass2	c:\ftp\share	RWLC	0
6	userz	pass3	c:\ftp\share	RL	0
7	sftpuser	userpass	c:\ftp\secure	RWDLC	0

5.6.2. Authenticating with LDAP Active Directory

Connections can be authenticated using Sysax LDAP Active Directory (Figure 5.16) by specifying the domain controller to use.

Figure 5.16. Authenticating with LDAP Active Directory



Multi Server Account Setup

User account selection

Connections can be authenticated using Sysax specific local accounts, LDAP Active Directory, windows NTLM, or ODBC databases (enterprise edition)

○ Use Database/ODBC Data Source for Authentication

● Use LDAP Active Directory Authentication

□ Set domain controller as Port 389

□ Use SSL to encrypt communication with domain controller

○ Use windows accounts for logging in users

○ Create Sysax user accounts

○ Use windows and Sysax user accounts. If username exists on both:

● Try logging into the windows account first

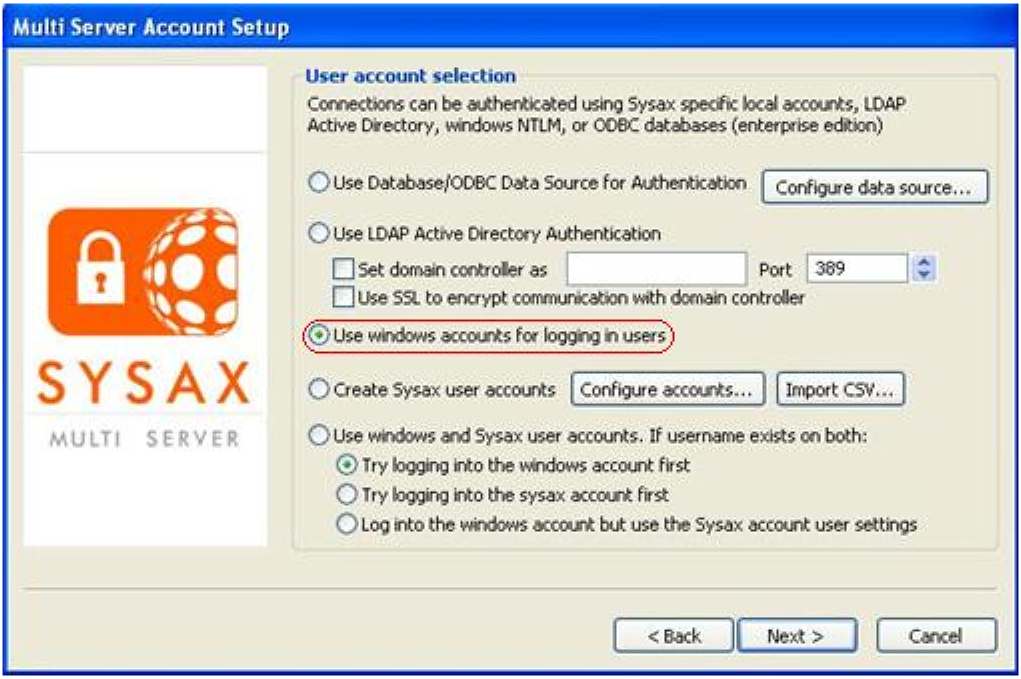
○ Try logging into the sysax account first

○ Log into the windows account but use the Sysax account user settings

5.6.3. Authenticating with Windows Accounts

Sysax server can use Windows accounts that have already been created on the computer system, or user accounts on a domain controller associated with the system. This enables system administrators to manage user accounts directly through the Windows computer management tools.

Figure 5.17. Authenticating with Windows Accounts



Multi Server Account Setup

User account selection

Connections can be authenticated using Sysax specific local accounts, LDAP Active Directory, windows NTLM, or ODBC databases (enterprise edition)

○ Use Database/ODBC Data Source for Authentication

○ Use LDAP Active Directory Authentication

□ Set domain controller as Port 389

□ Use SSL to encrypt communication with domain controller

● Use windows accounts for logging in users

○ Create Sysax user accounts

○ Use windows and Sysax user accounts. If username exists on both:

● Try logging into the windows account first

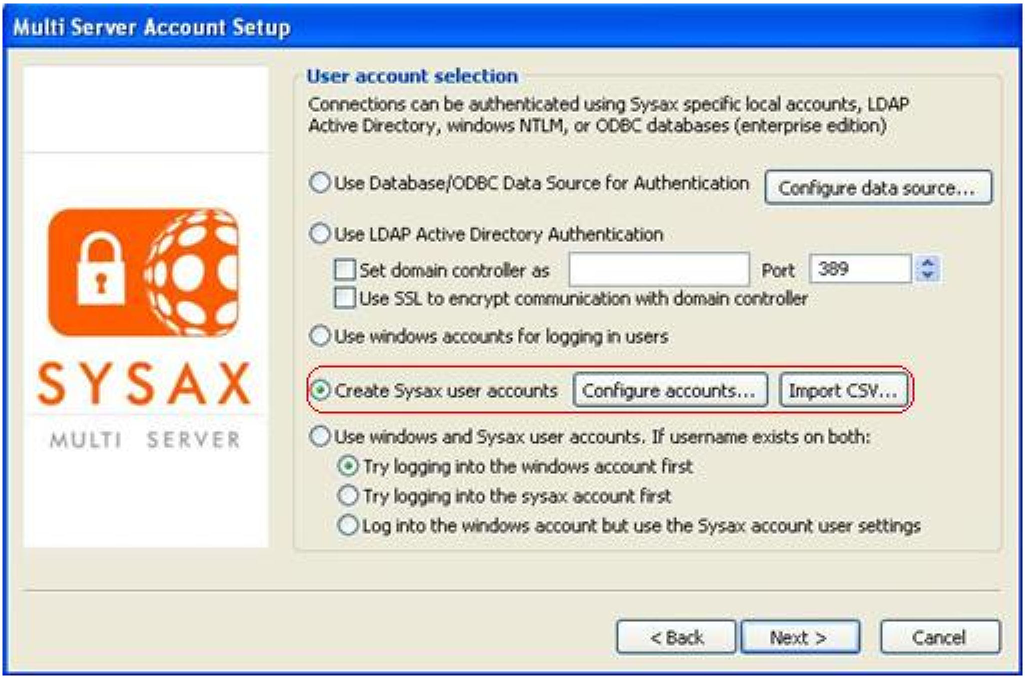
○ Try logging into the sysax account first

○ Log into the windows account but use the Sysax account user settings

5.6.4. Creating Sysax User Accounts

Sysax server specific user accounts can be created to enable account management directly through the Sysax server administration panel or through the web based administration interface.

Figure 5.18. User Account Selection with Sysax User Account Option



Connections can be authenticated using Sysax specific local accounts, LDAP Active Directory, windows NTLM, or ODBC databases (enterprise edition)

○ Use Database/ODBC Data Source for Authentication

○ Use LDAP Active Directory Authentication

□ Set domain controller as

Port 389

□ Use SSL to encrypt communication with domain controller

○ Use windows accounts for logging in users

● Create Sysax user accounts

○ Use windows and Sysax user accounts. If username exists on both:

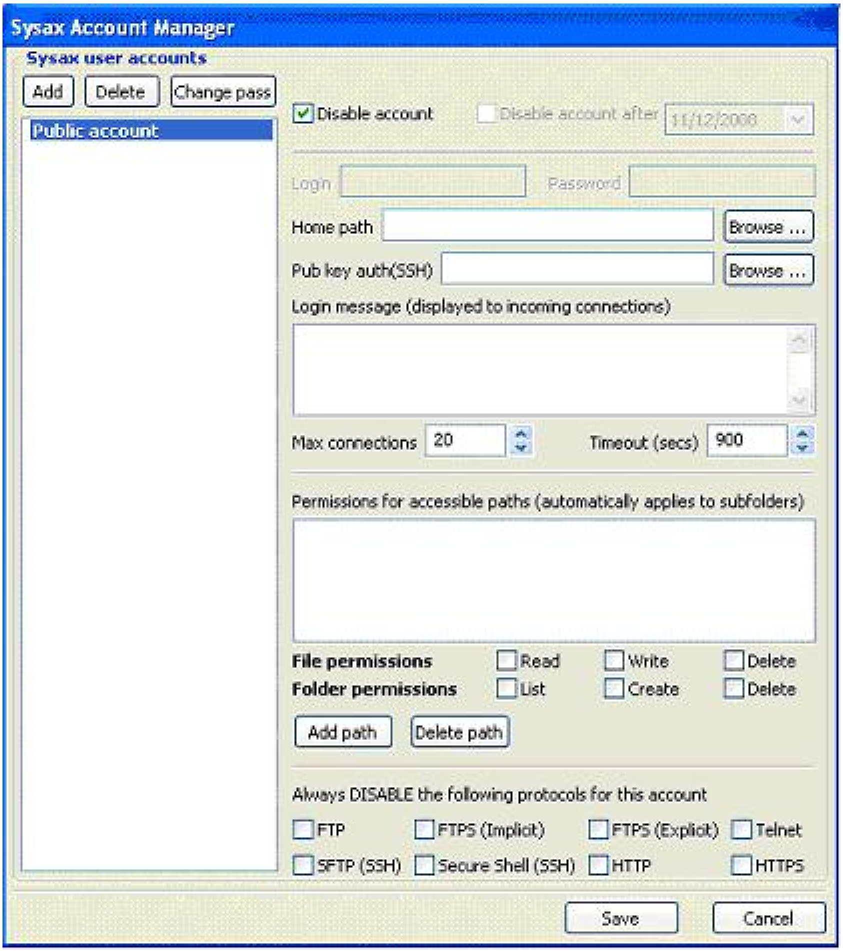
● Try logging into the windows account first

○ Try logging into the sysax account first

○ Log into the windows account but use the Sysax account user settings

Clicking on the **Configure accounts** button opens the Sysax account manager window where user accounts can be created, deleted, or modified.

Figure 5.19. System User Account Manager



Sysax Account Manager

Sysax user accounts

Public account

☑ Disable account

□ Disable account after 11/12/2008

Login

Password

Home path

Pub key auth(SSH)

Login message (displayed to incoming connections)

Max connections 20

Timeout (secs) 900

Permissions for accessible paths (automatically applies to subfolders)

File permissions	□ Read	□ Write	□ Delete
Folder permissions	□ List	□ Create	□ Delete

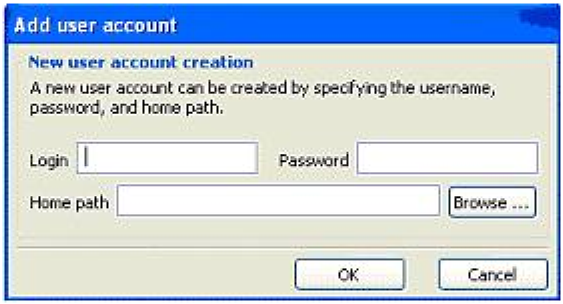
Always DISABLE the following protocols for this account

□ FTP	□ FTPS (Implicit)	□ FTPS (Explicit)	□ Telnet
□ SFTP (SSH)	□ Secure Shell (SSH)	□ HTTP	□ HTTPS

Adding User Accounts

The **Add User account** dialog box enables the creation of user accounts. A user account can be created by specifying the username, password and home path. In the Add user account dialog, the **Login** field is used to enter the user's login name. The **Password** field is used to enter the user's password. The **Home path** field is used to enter the home path for the user account. The **Browse** button can be clicked to quickly identify and select the home path. Finally click on the **OK** button to create the new user account.

Figure 5.20. Add User Account



Add user account

New user account creation

A new user account can be created by specifying the username, password, and home path.

Login

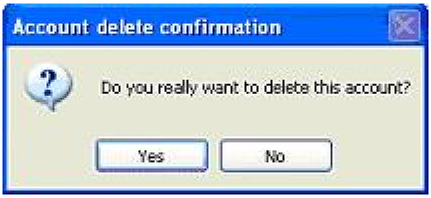
Password

Home path

Deleting User Accounts

When you choose to delete a user account, you are prompted by the **Account delete confirmation** screen.

Figure 5.21. Account Delete Confirmation



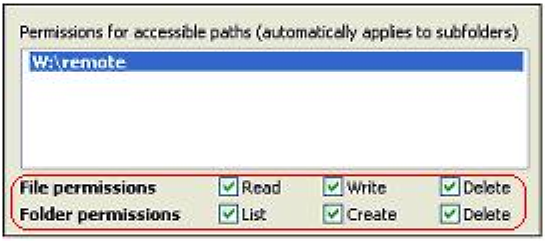
Account delete confirmation

Do you really want to delete this account?

This prevents you from inadvertently deleting an account. To verify the deletion, click **Yes**.

Granting User Permissions After you create the user accounts, the next step is to grant specific access permission for each account.

Figure 5.22. Setting Permissions



Permissions for accessible paths (automatically applies to subfolders)

W:\remote

File permissions ☑ Read ☑ Write ☑ Delete

Folder permissions ☑ List ☑ Create ☑ Delete

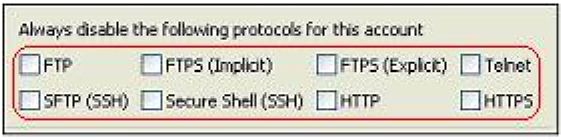
For each account listed in the field under **Permissions for accessible paths**, check the appropriate **file permissions(read/write/delete)** and **folder permissions(list/create/delete)**.

You can also use the **Add path** and **Delete path** buttons to add or delete the highlighted paths.

Disabling Specific Protocols

After granting the account permissions, the next step is to disable specific protocols for each account. To disable the specific protocols, check the appropriate protocols in this field.

Figure 5.23. Selecting User Protocols



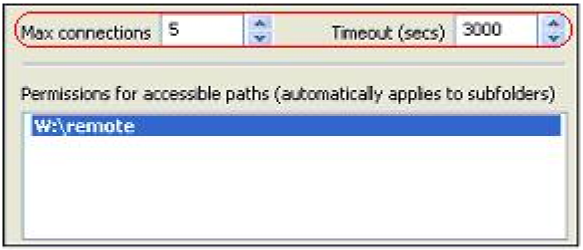
Always disable the following protocols for this account

□ FTP □ FTPS (Implicit) □ FTPS (Explicit) □ Telnet

□ SFTP (SSH) □ Secure Shell (SSH) □ HTTP □ HTTPS

Set Maximum Connections The figure below represents the screen that enables you to set the maximum number of connections allowed to connect to the FTP server. It also allows you to set a timeout period.

Figure 5.24. Maximum Connections and Timeout



Max connections: 5

Timeout (secs): 3000

Permissions for accessible paths (automatically applies to subfolders)

W:\remote

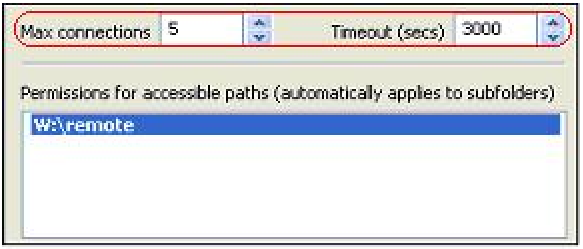
To set maximum connection and timeout period, enter the number in the field to the right of Max connections. You can also use the up and down arrows to select a number.

Set Timeout Period

If the Sysax Multi Server does not respond or does not finish a response in a timely manner after the client sends a command, the server times out and disconnects.

To reset the timeout specification, enter the appropriate seconds in the field to the right of Timeout(secs. You can also use the up and down arrows to select a number.

Figure 5.25. Maximum Connections and Timeout



Max connections 5 Timeout (secs) 3000

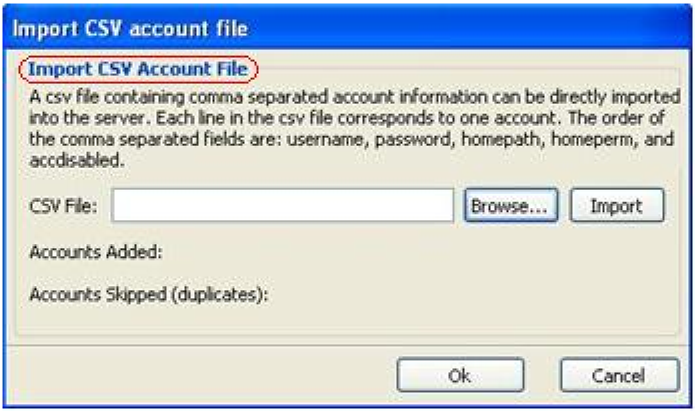
Permissions for accessible paths (automatically applies to subfolders)

W:\remote

5.6.5. Importing a CSV file containing Sysax User Accounts

Clicking on the **Import CSV** button opens the Import CSV account file window where a CSV file containing comma separated account information can be directly imported into the server.

Figure 5.26. Import CSV Account File



Import CSV account file

Import CSV Account File

A csv file containing comma separated account information can be directly imported into the server. Each line in the csv file corresponds to one account. The order of the comma separated fields are: username, password, homepath, homeperm, and accdisabled.

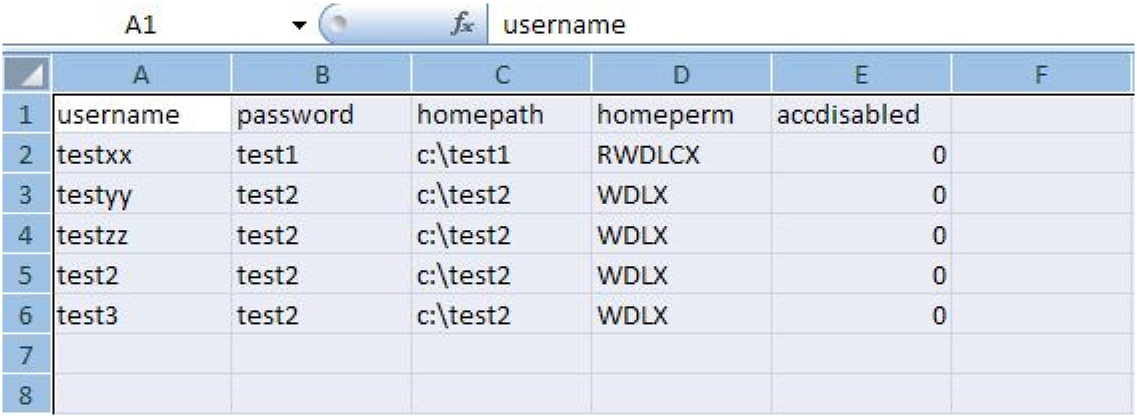
CSV File:

Accounts Added:

Accounts Skipped (duplicates):

Each line in the CSV file corresponds to one account. The orders of the comma separated fields are: 1.)username, 2.)password, 3.)homepath, 4.)homeperm and 5.)accdisabled. A sample CSV file is shown in below. The first row may optionally contain the field headings exactly as shown in the CSV file

Figure 5.27. Sample CSV File



	A	B	C	D	E	F
1	username	password	homepath	homeperm	accdisabled	
2	testxx	test1	c:\test1	RWDLCX	0	
3	testyy	test2	c:\test2	WDLX	0	
4	testzz	test2	c:\test2	WDLX	0	
5	test2	test2	c:\test2	WDLX	0	
6	test3	test2	c:\test2	WDLX	0	
7						
8						

In this,

- The **username** column contains the username for the account
- The **password** column contains the password for the account.
- The **homepath** column contains the home path for the account.
- The **homeperm** column contains the permissions for the home path and all sub folders.

For the permissions column, the following letters denote the following permissions:

R = file read

W = file write

D = file delete

L = folder list

C = folders create

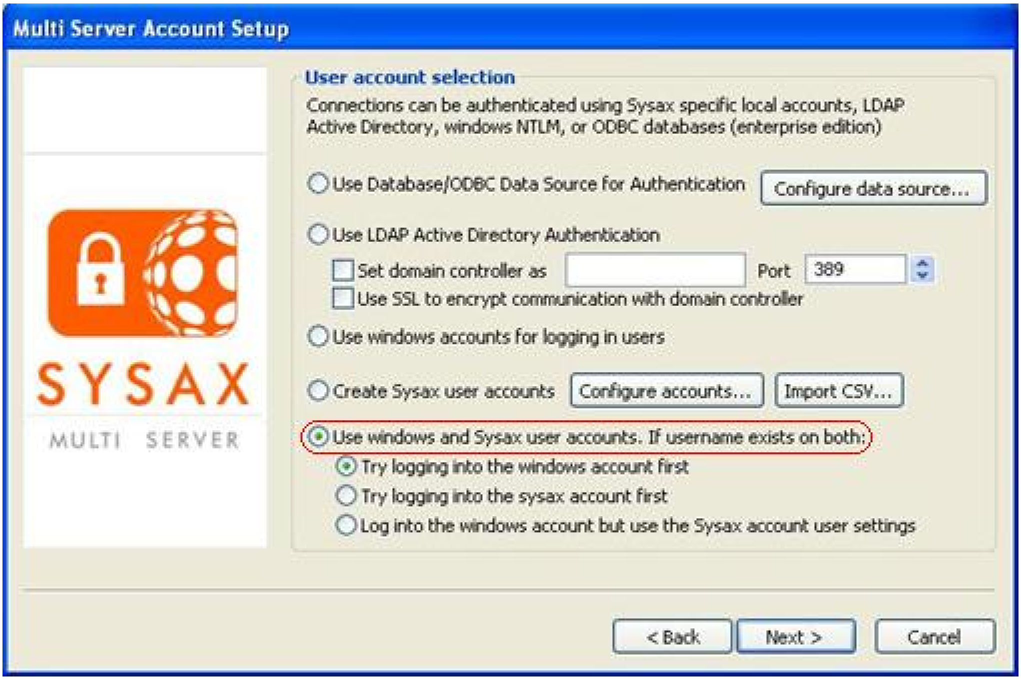
X = folder delete

The **accdisabled** column shows if the account is disabled. An account is disabled if this field is set to 1.

5.6.6. Using both Windows and Sysax User Accounts

It is also possible to authenticate users using a combination of either windows accounts or Sysax user accounts. If this option is selected and a username exists in both windows and Sysax user accounts, the server can be configured to use either Windows accounts or Sysax user accounts first to perform the authentication. The server may also be configured to login using the windows account and then use the sysax user settings.

Figure 5.28. Using both Windows and Sysax User Accounts



User account selection

Connections can be authenticated using Sysax specific local accounts, LDAP Active Directory, windows NTLM, or ODBC databases (enterprise edition)

○ Use Database/ODBC Data Source for Authentication

○ Use LDAP Active Directory Authentication

□ Set domain controller as Port 389

□ Use SSL to encrypt communication with domain controller

○ Use windows accounts for logging in users

○ Create Sysax user accounts

● Use windows and Sysax user accounts. If username exists on both:

● Try logging into the windows account first

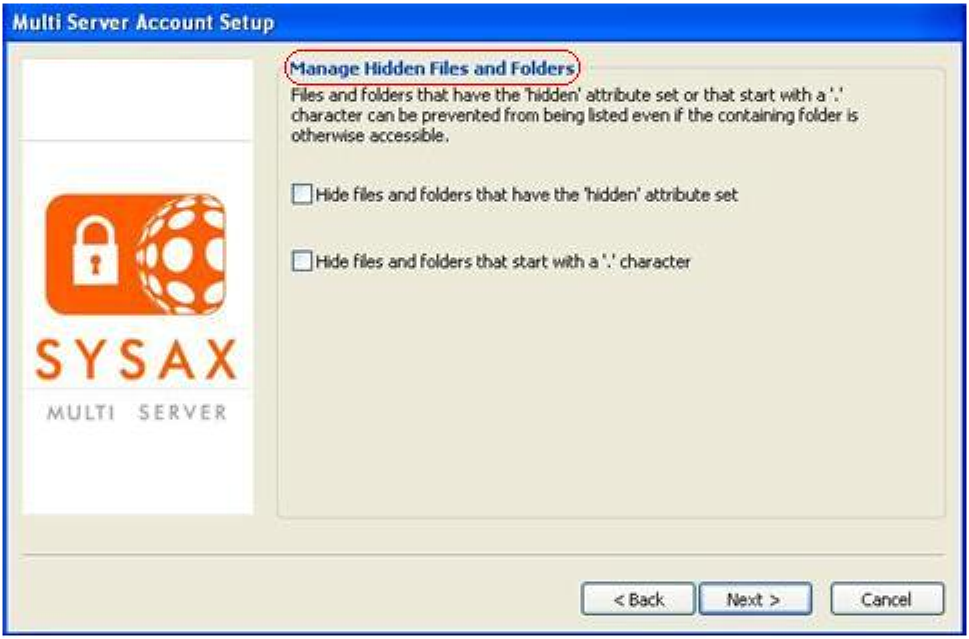
○ Try logging into the sysax account first

○ Log into the windows account but use the Sysax account user settings

5.7. Manage Hidden Files and Folders

Files and Folders that have the **'hidden'** attribute set or that start with a **'.'** character can be prevented from being listed even if the containing folder is otherwise accessible.

Figure 5.29. Manage Hidden Files and Folders



Manage Hidden Files and Folders

Files and folders that have the 'hidden' attribute set or that start with a '.' character can be prevented from being listed even if the containing folder is otherwise accessible.

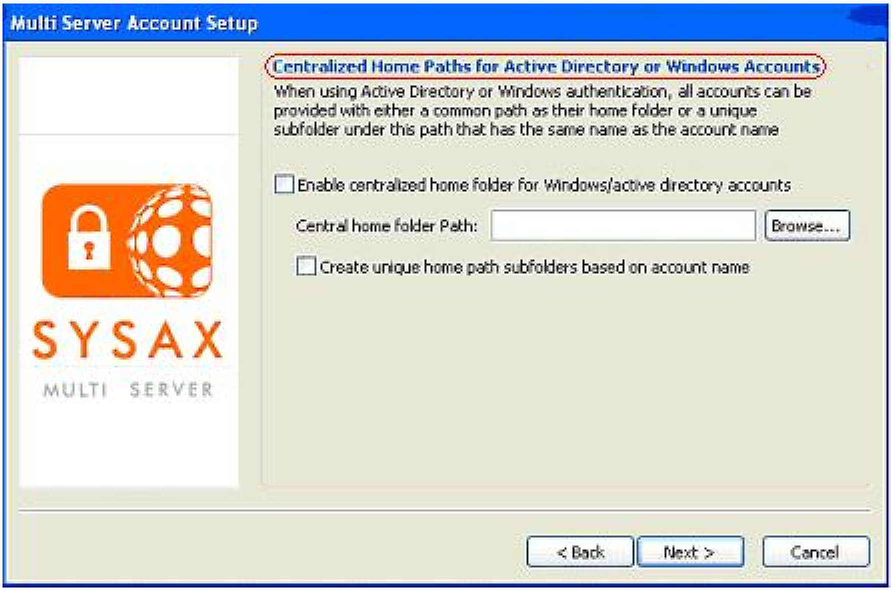
□ Hide files and folders that have the 'hidden' attribute set

□ Hide files and folders that start with a '.' character

5.8. Centralized Home Paths for Active Directory or Windows Accounts

When using Active Directory or Windows authentication in Sysax Server, all accounts can be provided with either a common path as their home folder or unique subfolder under this path that has the same name as the account name.

Figure 5.30. Centralized Home Paths for Active Directory or Windows Accounts



Centralized Home Paths for Active Directory or Windows Accounts

When using Active Directory or Windows authentication, all accounts can be provided with either a common path as their home folder or a unique subfolder under this path that has the same name as the account name

□ Enable centralized home folder for Windows/active directory accounts

Central home folder Path:

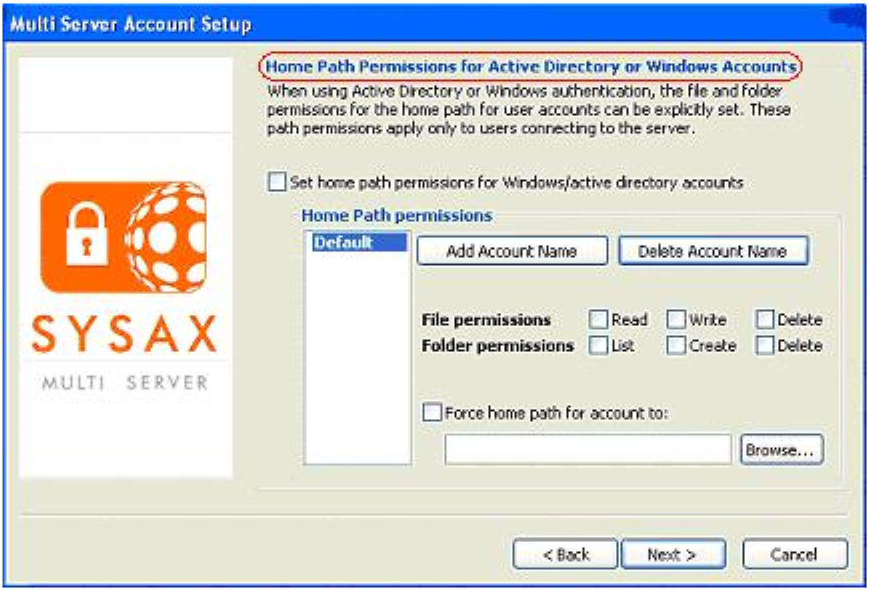
□ Create unique home path subfolders based on account name

In the "Centralized Home Paths for Active Directory or Windows Accounts" screen, select **Enable centralized home folder for Windows/active directory accounts** option to enable the centralized home folder for that account. You can click **Browse** from **Central home folder Path** field to quickly identify and select the home path. If you want to create unique home path subfolders, select **Create unique home path subfolders based on account name**.

5.9. Home Path Permissions for Active Directory or Windows Accounts

When using Active Directory or Windows authentication in Sysax Server, the file and folder permissions for the home path for user accounts can be explicitly set. These path permissions apply only to user connections to the server.

Figure 5.31. Home Path Permissions for Active Directory or Windows Accounts



Multi Server Account Setup

Home Path Permissions for Active Directory or Windows Accounts

When using Active Directory or Windows authentication, the file and folder permissions for the home path for user accounts can be explicitly set. These path permissions apply only to users connecting to the server.

□ Set home path permissions for Windows/active directory accounts

Home Path permissions

Default

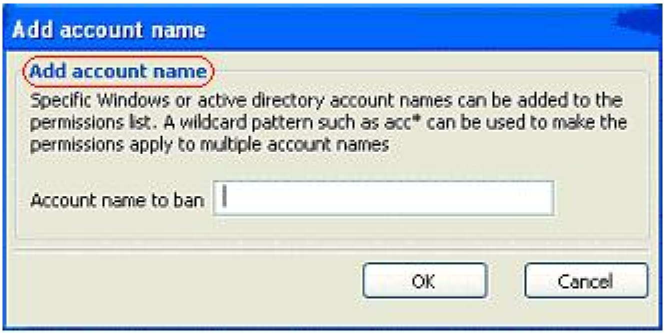
File permissions □ Read □ Write □ Delete

Folder permissions □ List □ Create □ Delete

□ Force home path for account to:

The **Home Path Permissions for Active Directory or Windows Accounts** screen, enables you to create and set file/folder permissions for windows/active directory accounts. An account name can be added by clicking on the **Add Account Name** button. To delete and account name, click **Delete Account Name** button. The Default account name is always present in the Home Path permissions field.

Figure 5.32. Add Account Name



Add account name

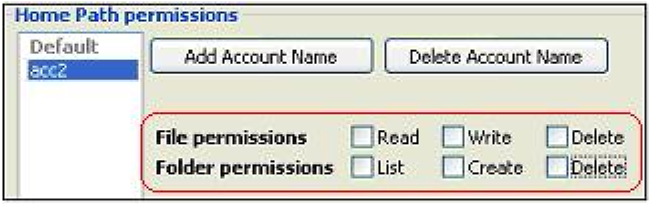
Add account name

Specific Windows or active directory account names can be added to the permissions list. A wildcard pattern such as acc* can be used to make the permissions apply to multiple account names

Account name to ban

After you add the windows/active directory accounts, the next step is to grant specific access permission for each account.

Figure 5.33. Add Account Name Permissions



File permissions □ Read □ Write □ Delete

Folder permissions □ List □ Create □ Delete

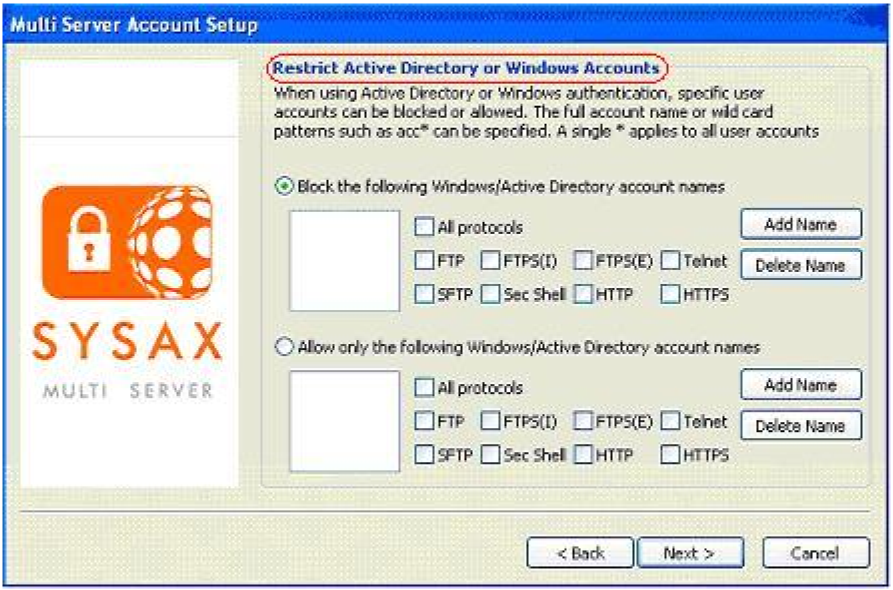
For each account name listed in the Home Path permissions field and then check the appropriate **file permissions(read/write/delete)** and **folder permissions(list/create/delete)**.

Also you can enable **Force home path for account to** and click **Browse** to quickly identify and select the force home path for account (Figure 5.31).

5.10. Restrict Active Directory or Windows Accounts

When using Active Directory or Windows authentication in Sysax Server, specific user accounts can be blocked or allowed. The full account name or wild card patterns such as acc* can be specified. A single * applies to all user accounts.

Figure 5.34. Restrict Active Directory or Windows Accounts



When using Active Directory or Windows authentication, specific user accounts can be blocked or allowed. The full account name or wild card patterns such as acc* can be specified. A single * applies to all user accounts

● Block the following Windows/Active Directory account names

□ All protocols

□ FTP □ FTPS(I) □ FTPS(E) □ Telnet

□ SFTP □ Sec Shell □ HTTP □ HTTPS

○ Allow only the following Windows/Active Directory account names

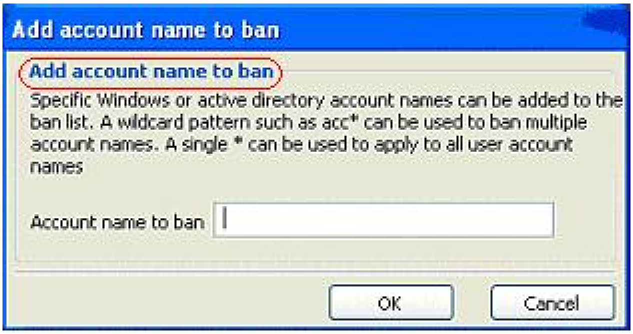
□ All protocols

□ FTP □ FTPS(I) □ FTPS(E) □ Telnet

□ SFTP □ Sec Shell □ HTTP □ HTTPS

To ban account names, select the **Block account names** radio box, Click on the **Add Name** button to add account names that need to be blocked.

Figure 5.35. Add Account Name to Ban

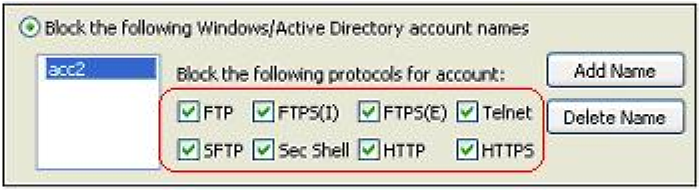


Specific Windows or active directory account names can be added to the ban list. A wildcard pattern such as acc* can be used to ban multiple account names. A single * can be used to apply to all user account names

Account name to ban

After adding the Window/Active Directory account name to ban, the next step is to block specific protocols for each account. To block the specific protocols, check the appropriate protocols in this filed.

Figure 5.36. Blocking Window/Active Directory Account Protocols



● Block the following Windows/Active Directory account names

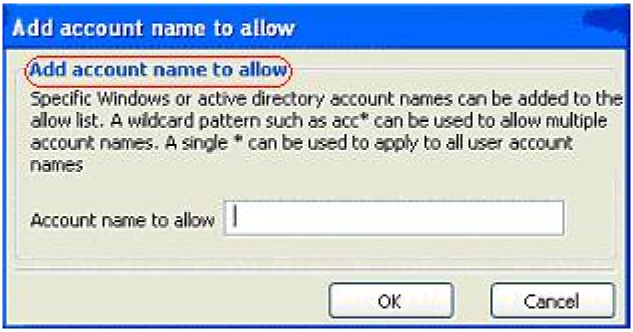
acc2

Block the following protocols for account:

☑ FTP ☑ FTPS(I) ☑ FTPS(E) ☑ Telnet
☑ SFTP ☑ Sec Shell ☑ HTTP ☑ HTTPS

To allow only specific account names, select the **Allow account names** radio box, Click on the **Add Name** button to add account names that need to be allowed.

Figure 5.37. Add Account Name to Allow

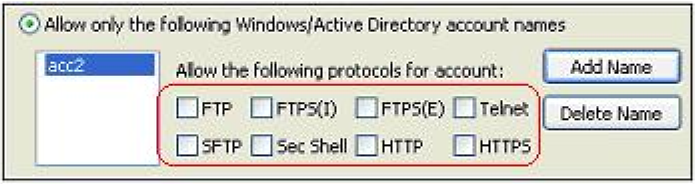


Specific Windows or active directory account names can be added to the allow list. A wildcard pattern such as acc* can be used to allow multiple account names. A single * can be used to apply to all user account names

Account name to allow

After adding the Window/Active Directory account name to allow, the next step is to **allow specific protocols** for each account. To allow the specific protocols, check the appropriate protocols in this filed.

Figure 5.38. Allowing Window/Active Directory Account Protocols



● Allow only the following Windows/Active Directory account names

acc2

Allow the following protocols for account:

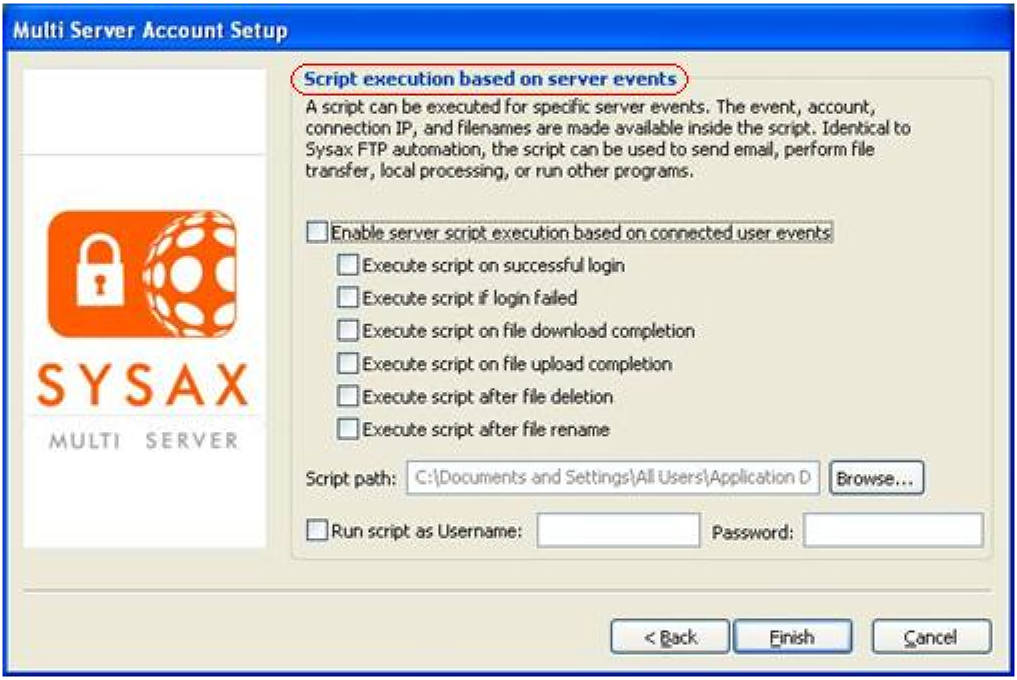
□ FTP □ FTPS(I) □ FTPS(E) □ Telnet

□ SFTP □ Sec Shell □ HTTP □ HTTPS

5.11. Running FTP Scripts Based on Server Events

Sysax Server enables the execution of custom scripts on specific server events. The event type, user account, connection IP address, and any filenames are made available inside the script. Identical to the scripting language used by the Sysax FTP Automation product, the script can be used to send email, perform file transfer, local processing, or run other programs.

Figure 5.39. Running FTP Scripts



Multi Server Account Setup

Script execution based on server events

A script can be executed for specific server events. The event, account, connection IP, and filenames are made available inside the script. Identical to Sysax FTP automation, the script can be used to send email, perform file transfer, local processing, or run other programs.

□ Enable server script execution based on connected user events

□ Execute script on successful login

□ Execute script if login failed

□ Execute script on file download completion

□ Execute script on file upload completion

□ Execute script after file deletion

□ Execute script after file rename

Script path: C:\Documents and Settings\All Users\Application D

□ Run script as Username: Password:

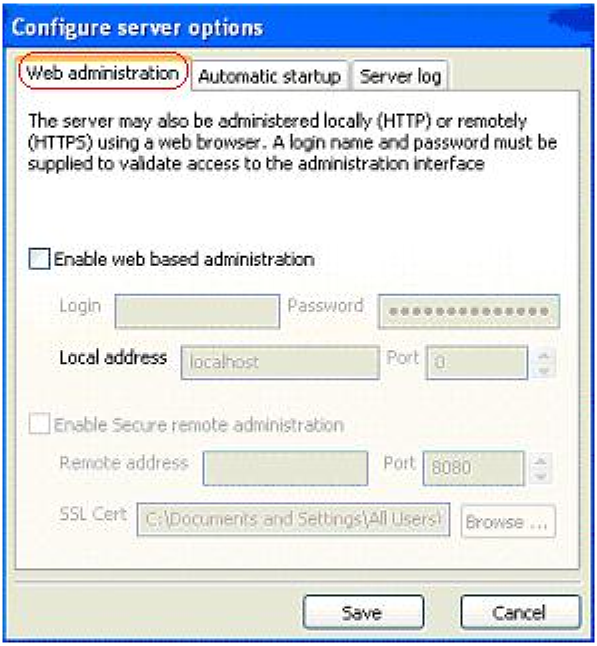
6

FTP Configuration

6.1. Setting-up Web-Based Administration

Sysax server can be administered locally (using HTTP)or remotely (using HTTPS) using a web browser. A username and password must be specified to validate access to the browser based administration interface.

Figure 6.1. Web Administration Interface



The server may also be administered locally (HTTP) or remotely (HTTPS) using a web browser. A login name and password must be supplied to validate access to the administration interface

□ Enable web based administration

Login:
Password: •••••••••••••••
Local address: localhost
Port: 0

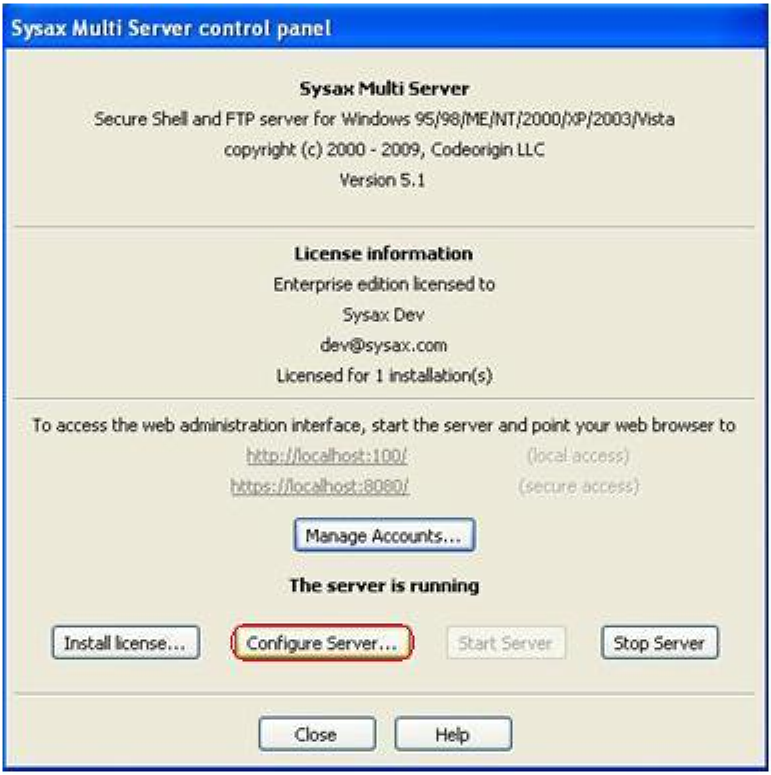
□ Enable Secure remote administration

Remote address:
Port: 8080
SSL Cert: C:\Documents and Settings\All Users\ Browse ...

6.2. Configuring Server Startup

To configure the server startup, open the Sysax Multi Server administrator program. The Sysax Multi server control panel is displayed(Figure 6.2).

Figure 6.2. Sysax Multi Server Control Panel



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

http://localhost:100/ (local access)

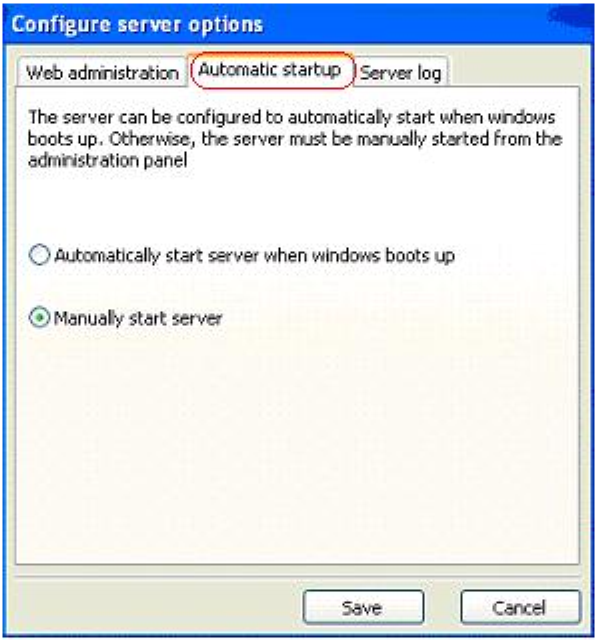
https://localhost:8080/ (secure access)

The server is running

On the automatic startup screen, you are presented with two options: to automatically start the server on Windows boot-up, or to start the server manually from the administrator panel.

Select the **appropriate startup method** and click **Save**. The following dialog box is displayed(Figure 6.3).

Figure 6.3. Configure Server Startup



The server can be configured to automatically start when windows boots up. Otherwise, the server must be manually started from the administration panel

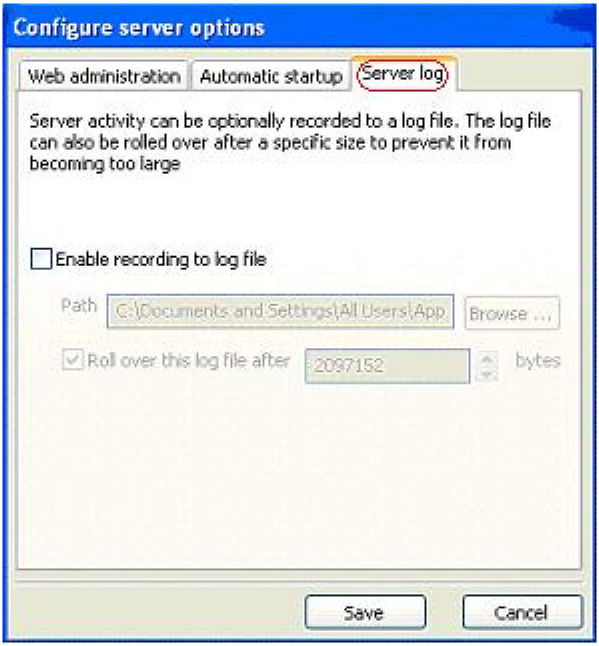
○ Automatically start server when windows boots up

● Manually start server

6.3. Configuring Server Logging

You can choose to optionally record server activity to a server log file. After you make your selections on the automatic startup screen and click **Save**, then select the **Server log tab**. The following dialog box is displayed(Figure 6.4).

Figure 6.4. Server Log



Configure server options

Server activity can be optionally recorded to a log file. The log file can also be rolled over after a specific size to prevent it from becoming too large

□ Enable recording to log file

Path C:\Documents and Settings\All Users\App

☑ Roll over this log file after 2097152 bytes

To enable recording of server activity to a logfile, make sure that the **Enable record to log file** is checked. Then enter the path in the Path field(or use the Browse button) to identify the log path.

In addition, on the Server log tab, you can indicate a maximum size of file that triggers a rollover to prevent the file from becoming too large.

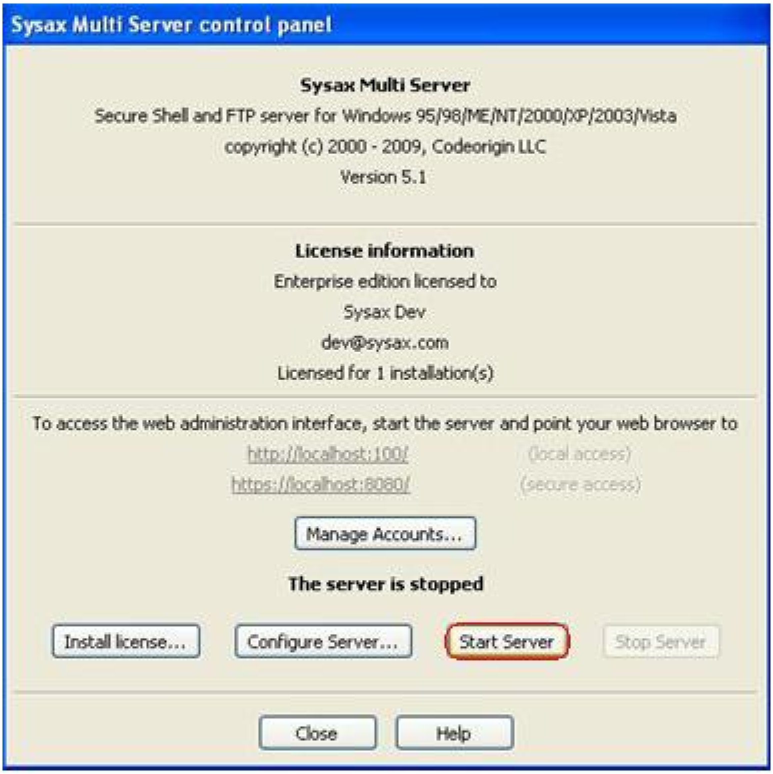
To specify the maximum size of the log file, verify that **Roll over this log file** after is checked(Figure 6.4), then enter the size in bytes(or use the up and down arrows). Finally click **Save** to preserve your settings.

7

How to start and stop Sysax Multi Server

After you establish a connection, you can start the server(Figure 7.1).

Figure 7.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is stopped

To start the server, follow these instructions:

1. Click **Start** button on task bar.

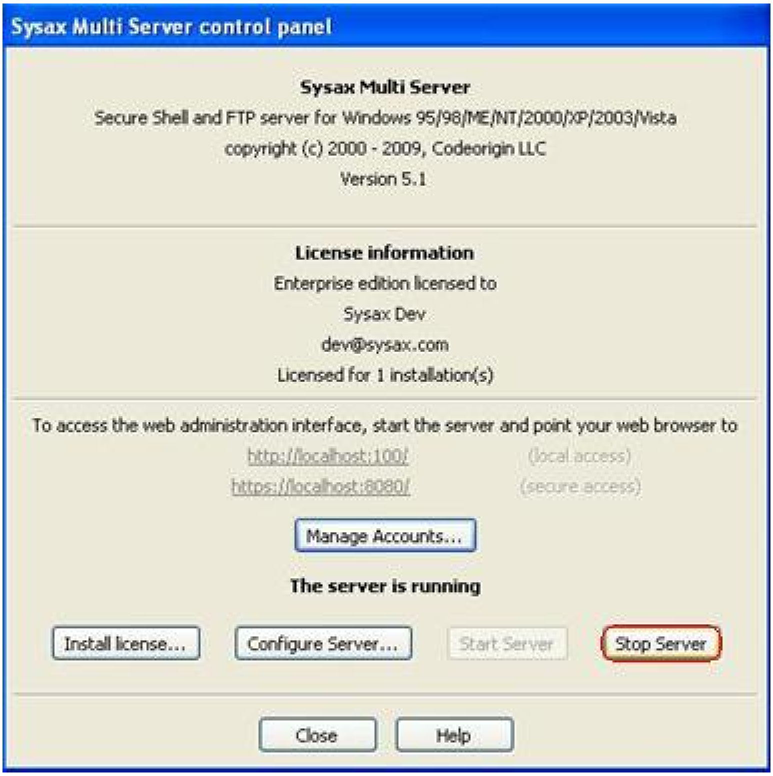
2. Select **Programs** -> **Sysax Multi Server**.

3. Click the sub-menu **Sysax Multi Server Administrator**.

4. Select **Start Server**.

After the server is used, you can stop its operation(Figure 7.2).

Figure 7.2. Stop Server



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is running

To stop the server, follow these instructions:

1. Click **Start** button on task bar.
2. Select **Programs** -> **Sysax Multi Server**.
3. Click the sub-menu **Sysax Multi Server Administrator**.
4. Select **Stop Server**.

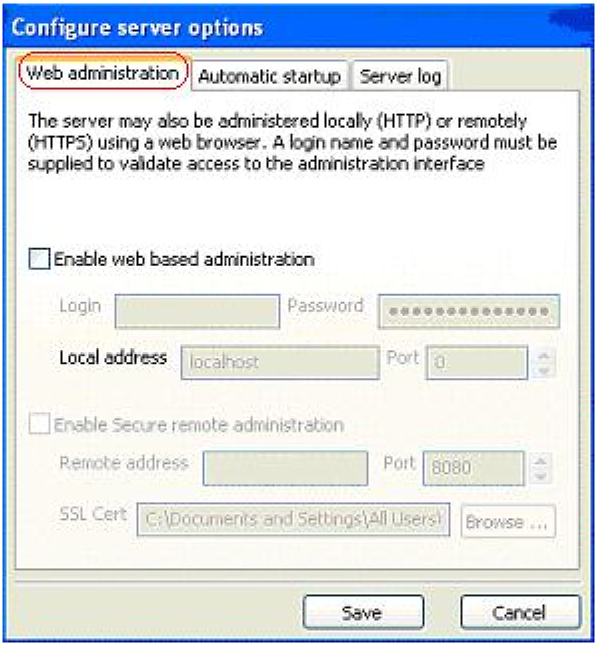
8

Using the web administration interface

On the web administration screen, you are presented with two check box options: to **Enable web based administration** and to **Enable server remote administration.**

Select the **appropriate web administration** option and click **Save**.See Figure 8.1 below.

Figure 8.1. Web Administration Interface



Configure server options

The server may also be administered locally (HTTP) or remotely (HTTPS) using a web browser. A login name and password must be supplied to validate access to the administration interface

□ Enable web based administration

Login

Password ●●●●●●●●●●●●●●

Local address localhost

Port 0

□ Enable Secure remote administration

Remote address

Port 8080

SSL Cert C:\Documents and Settings\All Users\

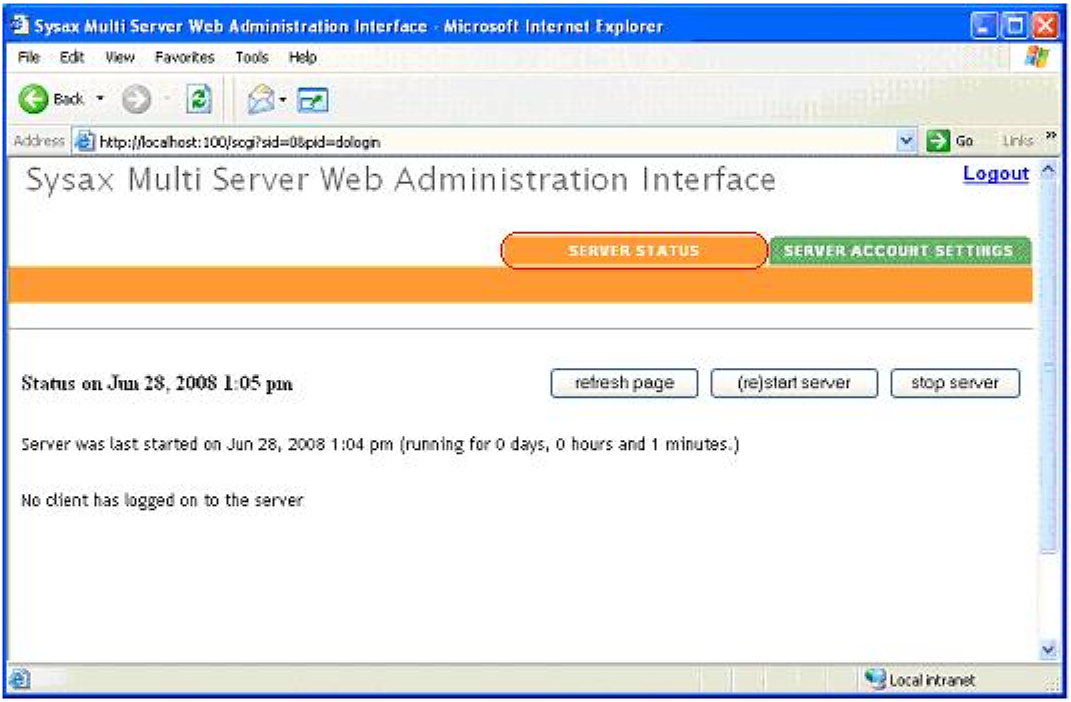
To **enable web administration** in Sysax Server, verify that enable web based administration is checked in web administration screen then **enter login name, password, local address** and **port**.

To **enable server remote administration** in Sysax Server, verify that enable server remote administration is checked in web administration screen. Enter **remote address, port** and the **path address** of SSL certificate, or click **Browse** to find the paths of remote and certificate.

8.1. Checking On Server Status in Real Time

When browsing or opening the Sysax Multi Server Web Administration Interface, the server status page is displayed(Figure 8.2).

Figure 8.2. Server Status Page


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Address
http://localhost:100/scgi?sid=0&pid=dologin
Go
Links
Sysax Multi Server Web Administration Interface
Logout
SERVER STATUS
SERVER ACCOUNT SETTINGS
refresh page
(re)start server
stop server
Local intranet

Status on Jun 28, 2008 1:05 pm

Server was last started on Jun 28, 2008 1:04 pm (running for 0 days, 0 hours and 1 minutes.)

No client has logged on to the server

The Server Status page shows the current status of server. It shows the month, date, year and time. It also shows the current running time of server and how many no of clients are connected to the server.

The opening page of Sysax Multi Server Web Administration Interface contains some different buttons.

- **Refresh Page**

  The refresh page button is used to refreshes the server status.

- **(Re)start Server**

  The (re)start server button is used to restart the server for new settings to take effect will disconnect all connected users.

- **Stop Server**

  The stop server button is used to stop the server.

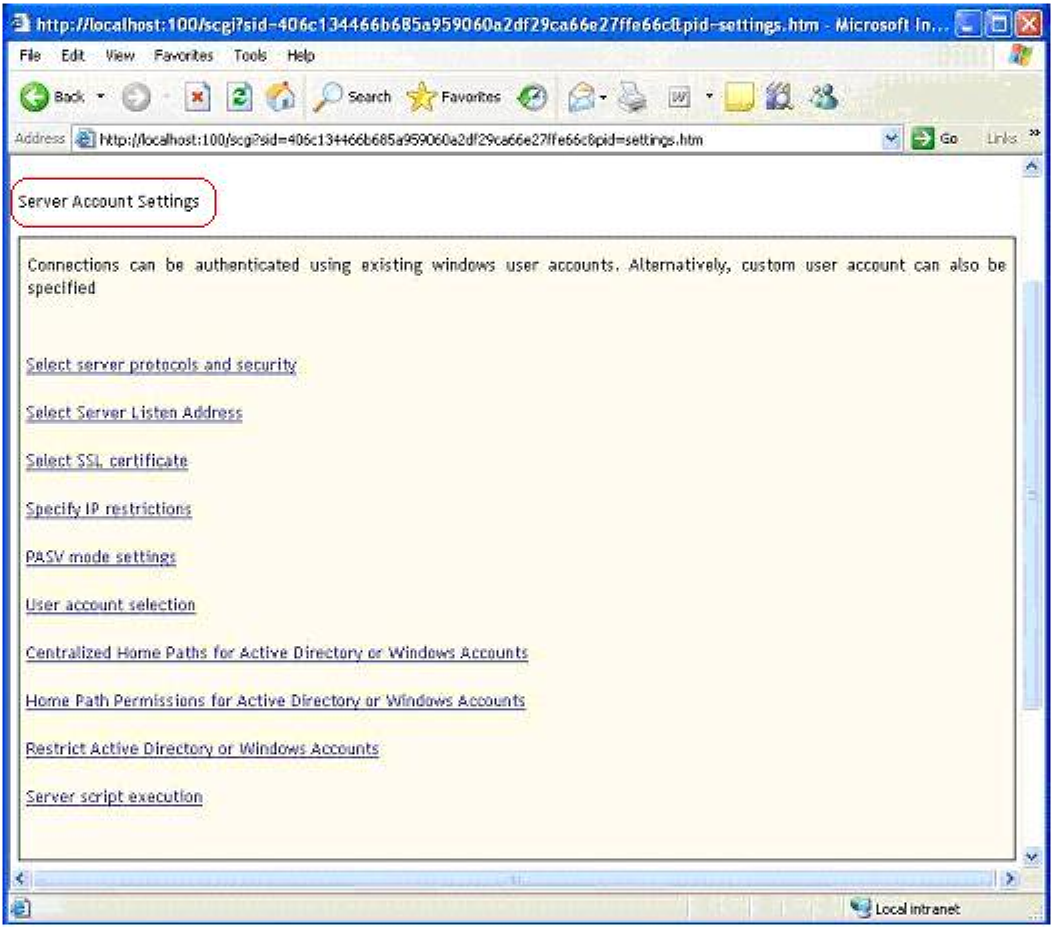
- **Logout**

  The logout button is used to logout the currently used working account.

8.2. Updating Server Settings using Web Interface

To **update server settings**, select **Server account settings** tab of Sysax Multi Server Web Administration Interface window. The server account settings page is displayed in figure 8.3.

Figure 8.3. Updating Server Settings using Web Interface


http://localhost:100/scgi?sid-406c134466b685a959060a2df29ca66e27ffe66c8pid-settings.htm - Microsoft In...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://localhost:100/scgi?sid=406c134466b685a959060a2df29ca66e27ffe66c8pid=settings.htm
Go
Links
Local intranet

Server Account Settings

Connections can be authenticated using existing windows user accounts. Alternatively, custom user account can also be specified

Select server protocols and security

Select Server Listen Address

Select SSL certificate

Specify IP restrictions

PASV mode settings

User account selection

Centralized Home Paths for Active Directory or Windows Accounts

Home Path Permissions for Active Directory or Windows Accounts

Restrict Active Directory or Windows Accounts

Server script execution

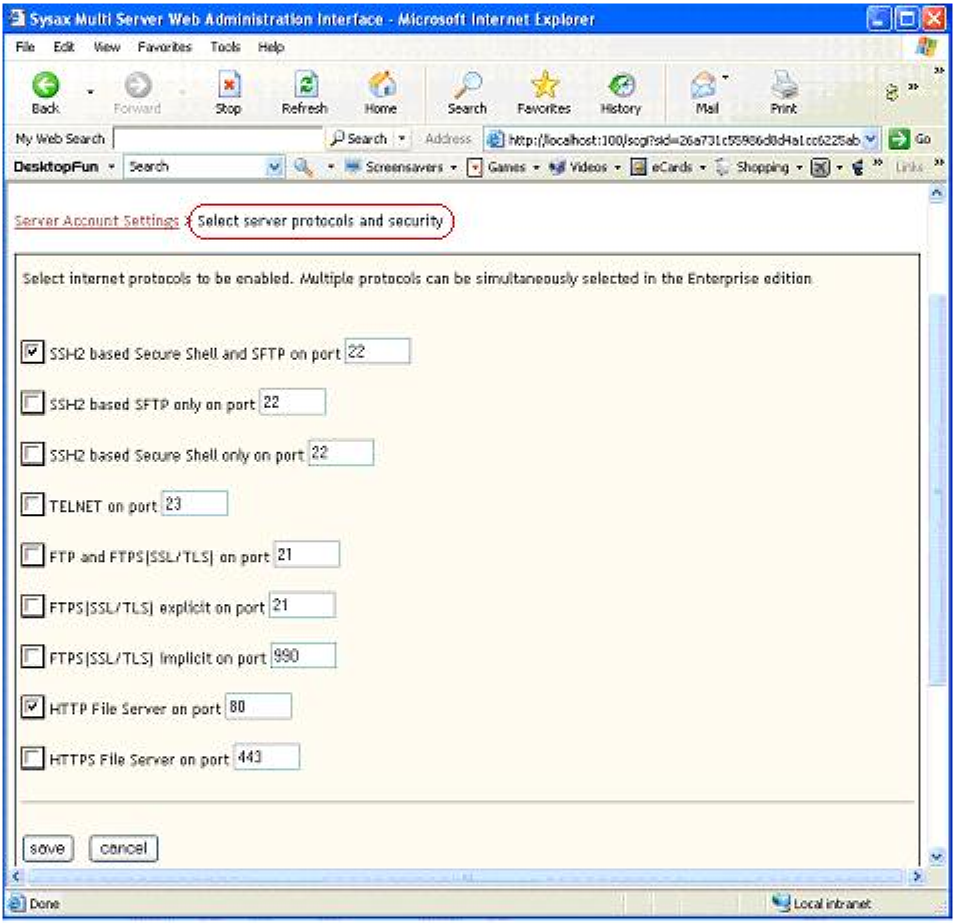
You can update the server settings by using web browser. Select the appropriate server settings option of server account settings page in Sysax Multi Server web administration interface.

8.2.1. Selecting Internet Protocols and Security

To update the **selecting server protocol** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.
- Pick **Select server protocols and security** option.
- Then **update** the settings.
- Finally, click **Save** button to save the server current settings.

Figure 8.4. Selecting Internet Protocols and Security


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
My Web Search Search Address http://localhost:100/scgi?sid=26a731c55986d8d4a1cc6225ab Go
DesktopFun Search Screensavers Games Videos eCards Shopping Links
Done
Local intranet

Server Account Settings › Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

☑ SSH2 based Secure Shell and SFTP on port 22

☐ SSH2 based SFTP only on port 22

☐ SSH2 based Secure Shell only on port 22

☐ TELNET on port 23

☐ FTP and FTPS(SSL/TLS) on port 21

☐ FTPS(SSL/TLS) explicit on port 21

☐ FTPS(SSL/TLS) implicit on port 990

☑ HTTP File Server on port 80

☐ HTTPS File Server on port 443

8.2.2. Selecting Server Listen Address

To update the **server listen address** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Click on **Select Server Listen address** tab.
- Select any one of the option.

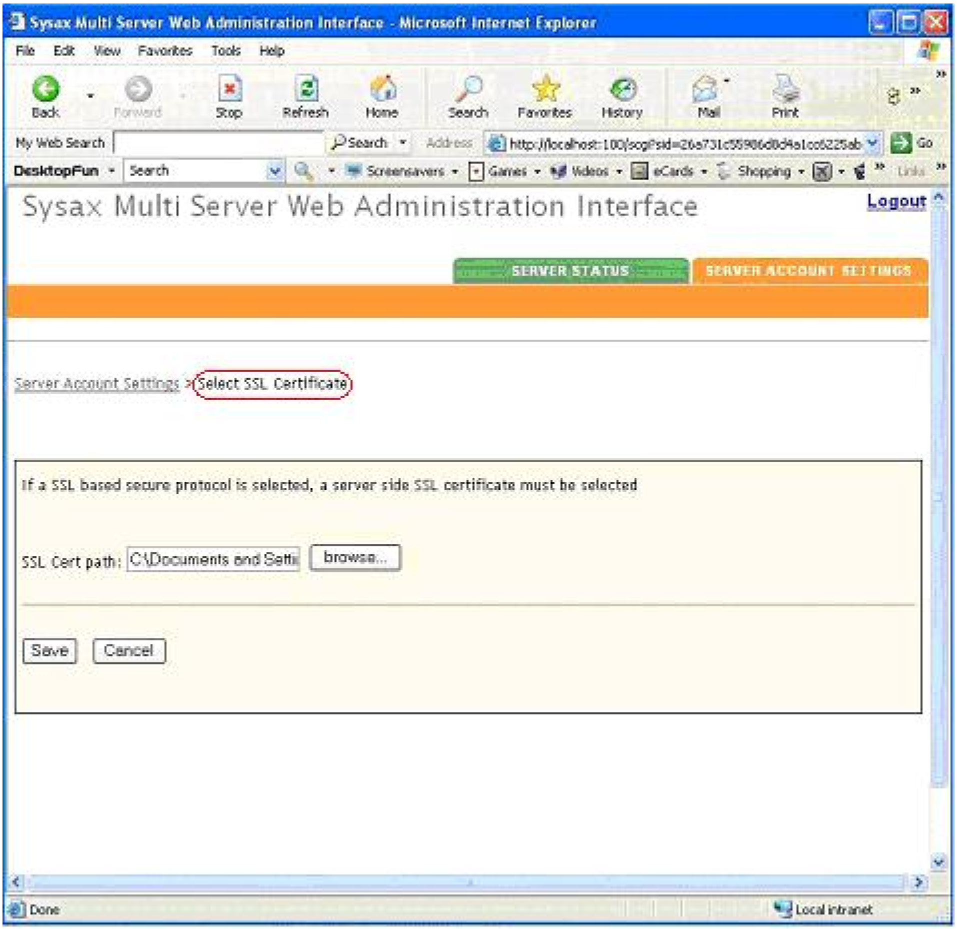
Figure 8.5. Selecting Server Listen Address

8.2.3. Selecting SSL Certificate

To update the **selecting ssl certificate** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.
- Pick **Select SSL Certificate** option.
- Then **update** the settings.
- Finally, click **Save** button to save the server current settings.

Figure 8.6. Selecting SSL Certificate


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
My Web Search
Search
Address http://localhost:100/scgi?sid=26a731c55986d8d4a1cc6225ab
Go
DesktopFun Search Screensavers Games Videos eCards Shopping
Links
Sysax Multi Server Web Administration Interface
Logout
SERVER STATUS
SERVER ACCOUNT SETTINGS
Server Account Settings > Select SSL Certificate
browse...
Save
Cancel
Done
Local intranet

If a SSL based secure protocol is selected, a server side SSL certificate must be selected

SSL Cert path: C:\Documents and Setti

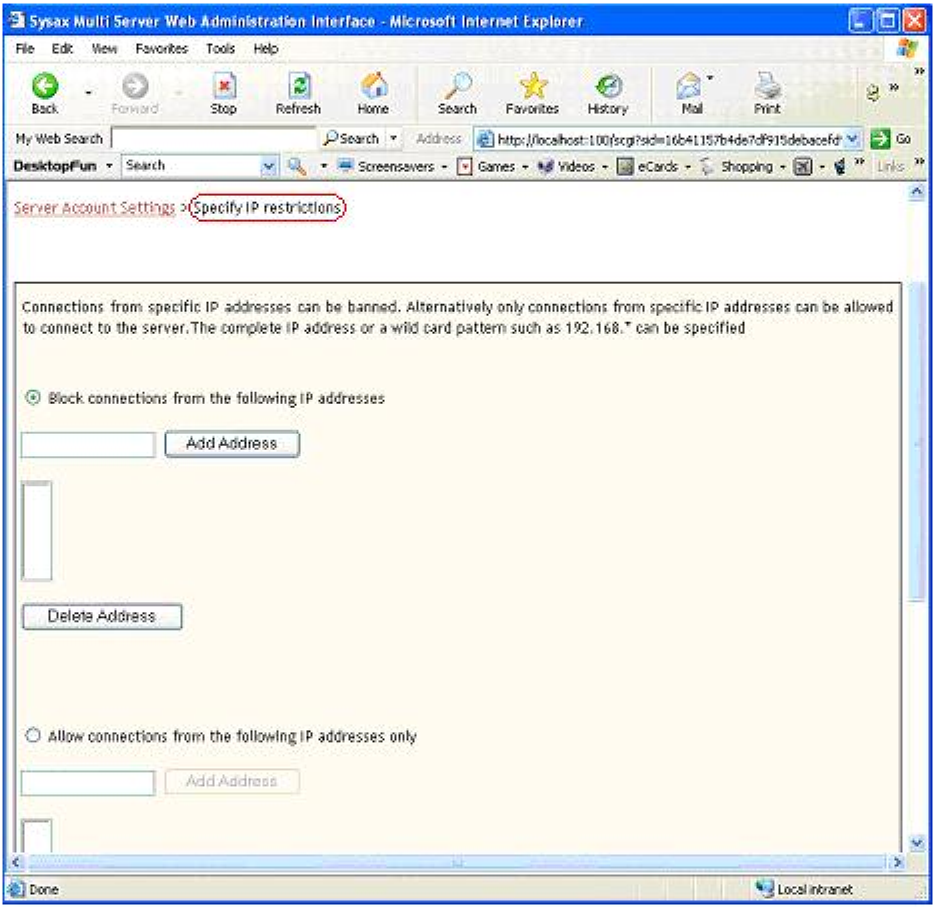
8.2.4. Specifying IP Restrictions

To update the **specifying IP restrictions** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.
- Pick **Specify IP restrictions** option.
- Then **update** the settings.

- Finally, click **Save** button to save the server current settings.

Figure 8.7. Specifying IP Restrictions



Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
My Web Search
Search
Address http://localhost:100/scgi?sid=16b41157b4de7df915debacefd
Go
DesktopFun Search Screensavers Games Videos eCards Shopping Links
Add Address
Delete Address
Add Address
Done
Local intranet

Server Account Settings > Specify IP restrictions

Connections from specific IP addresses can be banned. Alternatively only connections from specific IP addresses can be allowed to connect to the server.The complete IP address or a wild card pattern such as 192.168.* can be specified

● Block connections from the following IP addresses

○ Allow connections from the following IP addresses only

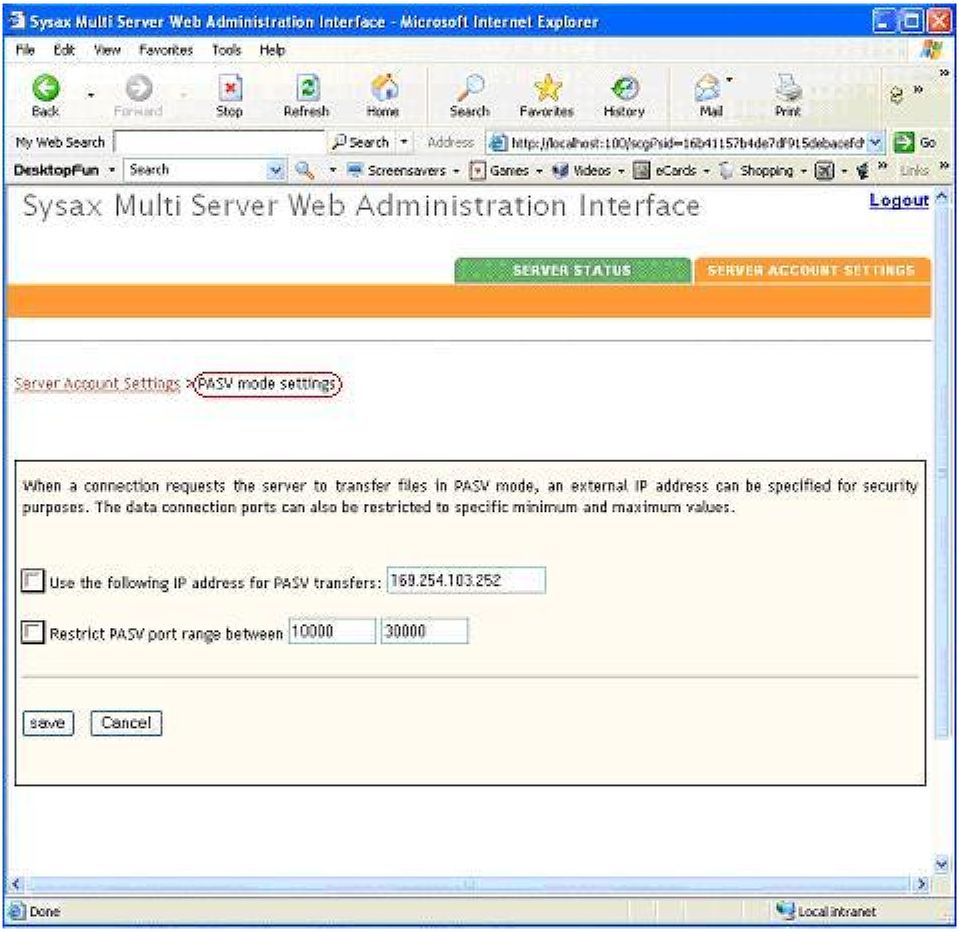
8.2.5. PASV Mode Settings

To update the **PASV mode settings** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.
- Pick **PASV mode settings** option.
- Then **update** the settings.

- Finally, click **Save** button to save the server current settings.

Figure 8.8. Setting PASV Mode


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
My Web Search
Search
Address
http://localhost:100/scgi?sid=16b41157b4de7df915debacefd
Go
DesktopFun
Search
Screensavers Games Videos eCards Shopping
Links
Sysax Multi Server Web Administration Interface
Logout
SERVER STATUS
SERVER ACCOUNT SETTINGS
Server Account Settings >PASV mode settings
save
Cancel
Done
Local intranet

When a connection requests the server to transfer files in PASV mode, an external IP address can be specified for security purposes. The data connection ports can also be restricted to specific minimum and maximum values.

□ Use the following IP address for PASV transfers: 169.254.103.252

□ Restrict PASV port range between 10000 30000

8.2.6. User Account Selections

To update the **user account selection** page of Sysax Multi Server Web Administration Interface, follow these instructions:

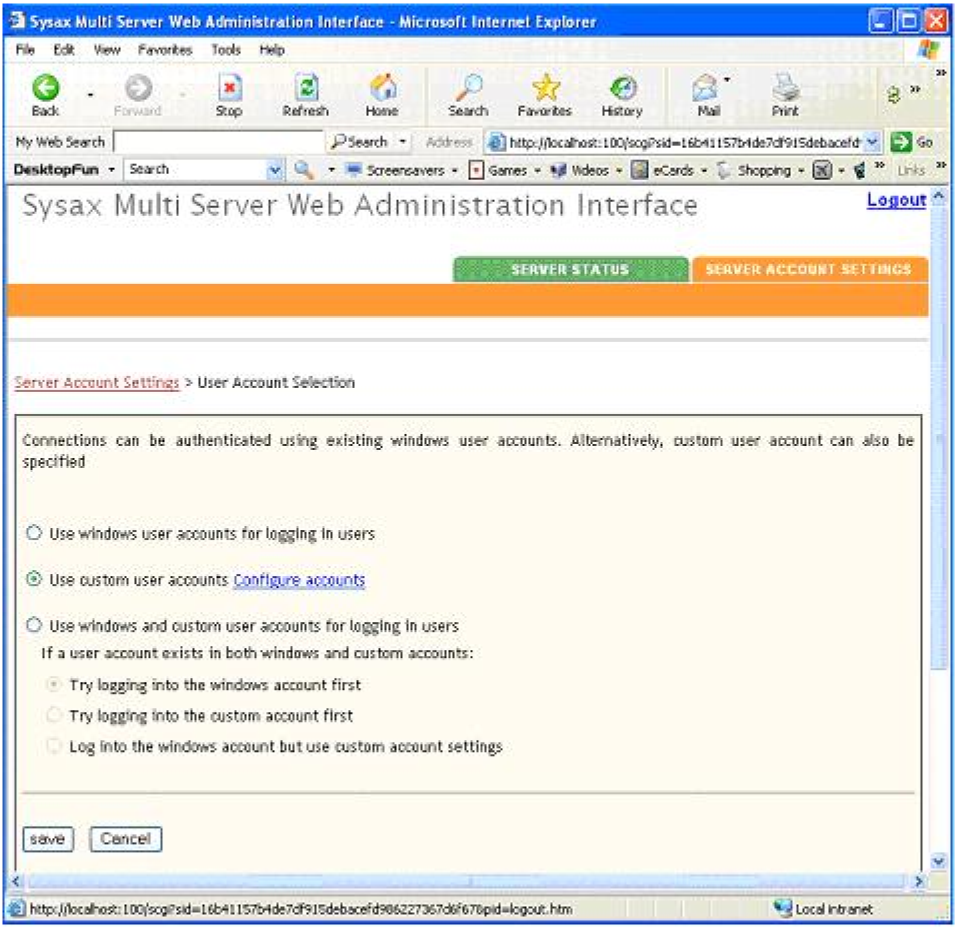
- Select **Server Account Settings** tab.

- Pick **User Account Selection** option.

- Then **update** the settings.

- Finally, click **Save** button to save the server current settings.

Figure 8.9. User Account Selections


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
My Web Search Search Address http://localhost:100/scgi?sid=16b41157b4de7df915debacefd Go
DesktopFun Search Screensavers Games Videos eCards Shopping Links
Sysax Multi Server Web Administration Interface
Logout
SERVER STATUS
SERVER ACCOUNT SETTINGS
Server Account Settings > User Account Selection
save
Cancel
http://localhost:100/scgi?sid=16b41157b4de7df915debacefd986227367d6f67&pid=logout.htm
Local intranet

Connections can be authenticated using existing windows user accounts. Alternatively, custom user account can also be specified

○ Use windows user accounts for logging in users

● Use custom user accounts Configure accounts

○ Use windows and custom user accounts for logging in users

If a user account exists in both windows and custom accounts:

● Try logging into the windows account first

○ Try logging into the custom account first

○ Log into the windows account but use custom account settings

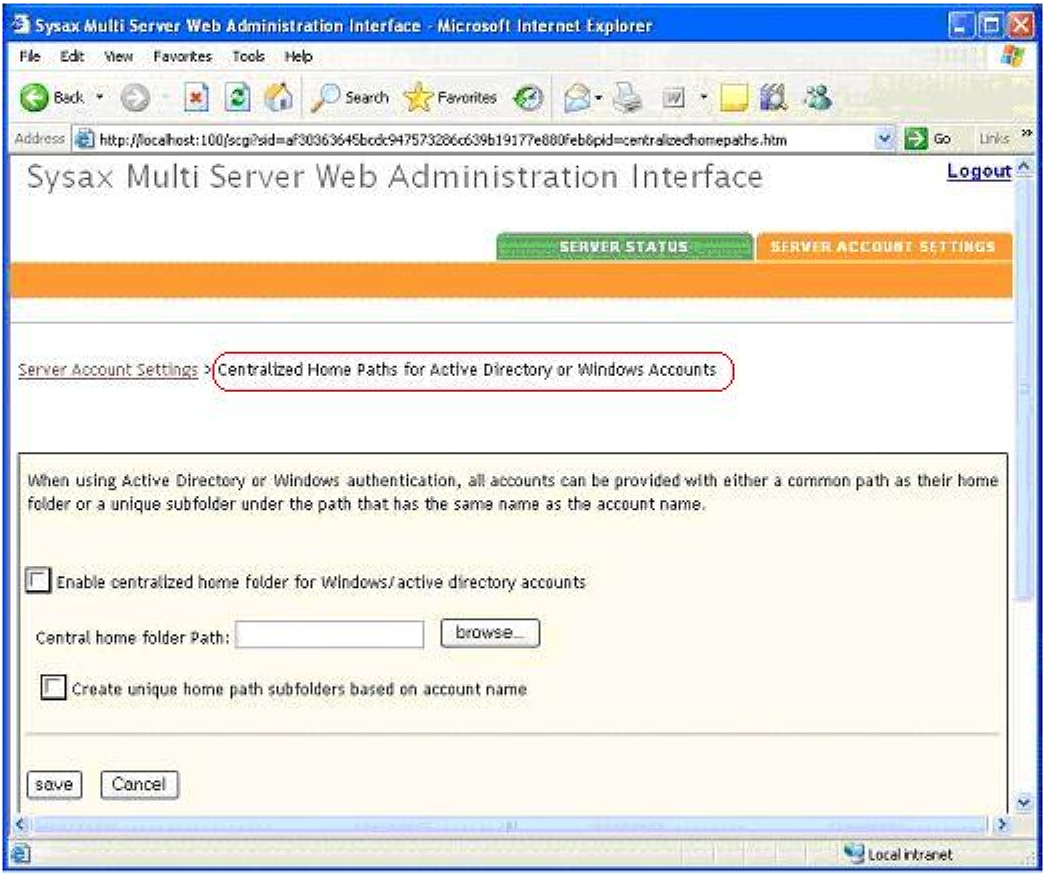
8.2.7. Centralized Home Paths for Active Directory or Windows Accounts

To update the **centralized home paths selection** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.

- Pick **Centralized Home Paths for Active Directory or Windows Accounts** option.
- Then **update** the settings.
- Finally, click **Save** button to save the server current settings.

Figure 8.10. Centralized Home Paths Selections



Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer

http://localhost:100/scgi?sid=af30363645bcdc947573286c639b19177e880feb6pid=centralizedhomepaths.htm

Sysax Multi Server Web Administration Interface

Server Account Settings > Centralized Home Paths for Active Directory or Windows Accounts

When using Active Directory or Windows authentication, all accounts can be provided with either a common path as their home folder or a unique subfolder under the path that has the same name as the account name.

□ Enable centralized home folder for Windows/active directory accounts

Central home folder Path:

□ Create unique home path subfolders based on account name

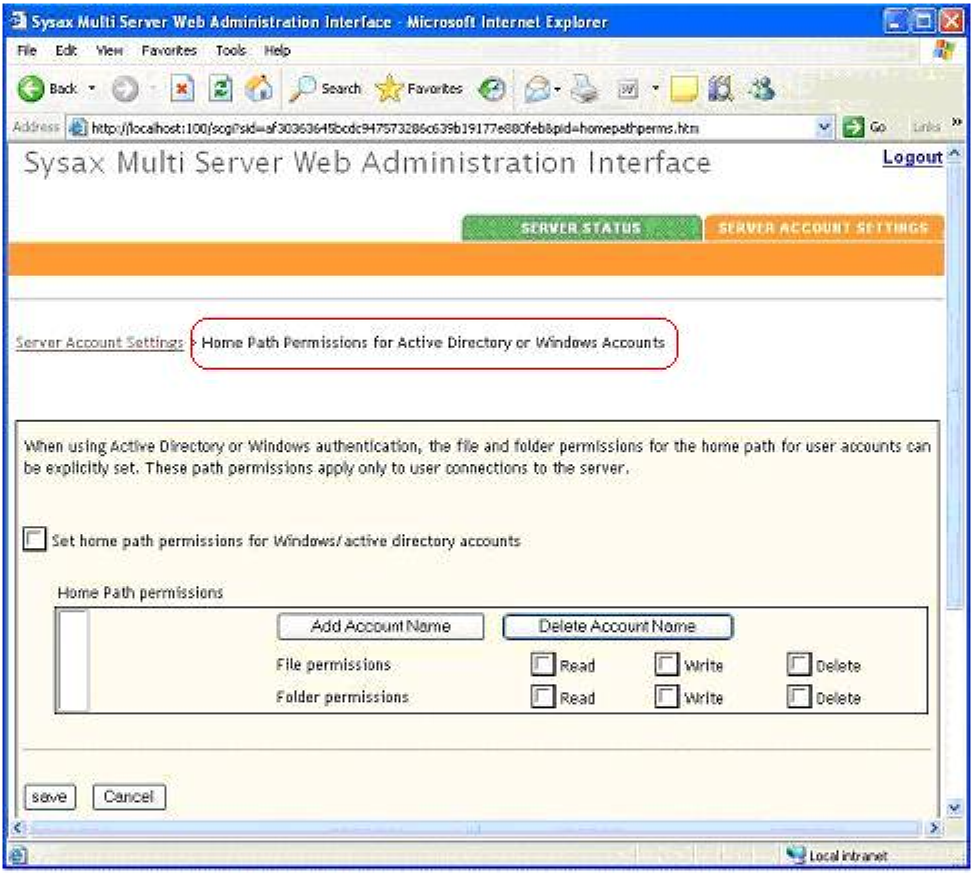
8.2.8. Home Path Permissions for Active Directory or Windows Accounts

To update the **home path permissions selection** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.

- Pick **Home Path Permissions for Active Directory or Windows Accounts** option.
- Then **update** the settings.
- Finally, click **Save** button to save the server current settings.

Figure 8.11. Home Path Permissions Selections


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://localhost:100/scgi?sid=af30363645bcdc947573286c639b19177e880feb&pid=homepathperms.htm
Go
Links
Sysax Multi Server Web Administration Interface
Logout
SERVER STATUS
SERVER ACCOUNT SETTINGS
Server Account Settings
Home Path Permissions for Active Directory or Windows Accounts
Home Path permissions
Add Account Name
Delete Account Name
save
Cancel
Local intranet

When using Active Directory or Windows authentication, the file and folder permissions for the home path for user accounts can be explicitly set. These path permissions apply only to user connections to the server.

□ Set home path permissions for Windows/active directory accounts

File permissions □ Read □ Write □ Delete

Folder permissions □ Read □ Write □ Delete

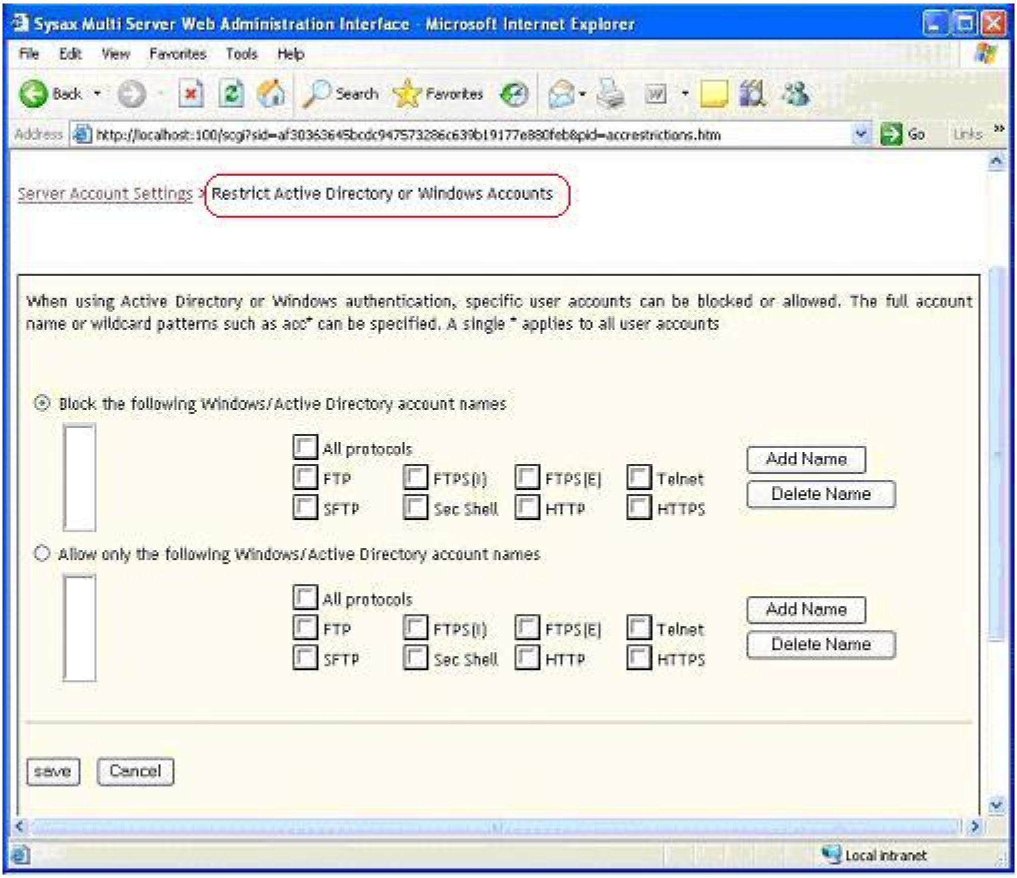
8.2.9. Restrict Active Directory or Windows Accounts

To update the **restrict accounts selection** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.

- Pick **Restrict Active Directory or Windows Accounts** option.
- Then **update** the settings.
- Finally, click **Save** button to save the server current settings.

Figure 8.12. Restrict Accounts Selections


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Local intranet

http://localhost:100/scgi?sid=af30363645bcdc947573286c639b19177e880feb&pid=accrestrictions.htm

Server Account Settings > Restrict Active Directory or Windows Accounts

When using Active Directory or Windows authentication, specific user accounts can be blocked or allowed. The full account name or wildcard patterns such as acc* can be specified. A single * applies to all user accounts

● Block the following Windows/Active Directory account names

□ All protocols
□ FTP □ FTPS(I) □ FTPS(E) □ Telnet
□ SFTP □ Sec Shell □ HTTP □ HTTPS

Add Name
Delete Name

○ Allow only the following Windows/Active Directory account names

□ All protocols
□ FTP □ FTPS(I) □ FTPS(E) □ Telnet
□ SFTP □ Sec Shell □ HTTP □ HTTPS

Add Name
Delete Name

save Cancel

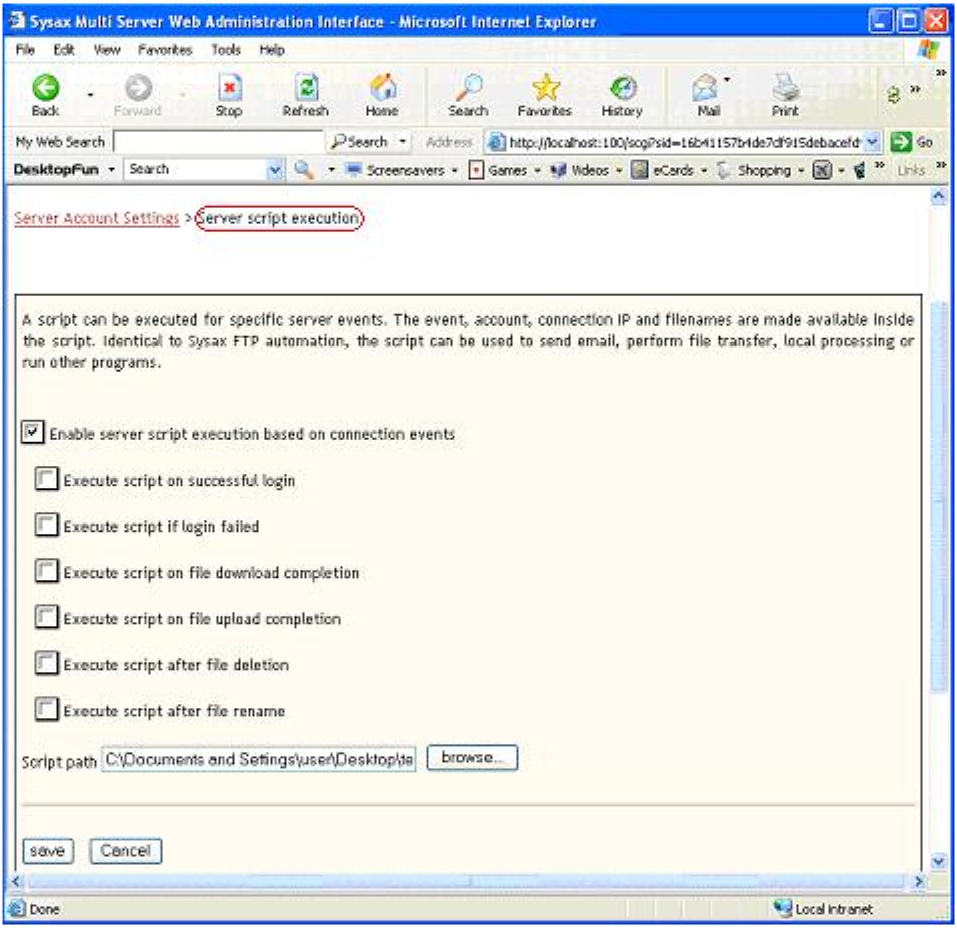
8.2.10. Server Script Execution

To update the **server script execution** page of Sysax Multi Server Web Administration Interface, follow these instructions:

- Select **Server Account Settings** tab.

- Pick **Server script execution** option.
- Then **update** the settings.
- Finally, click **Save** button to save the server current settings.

Figure 8.13. Server script execution


Sysax Multi Server Web Administration Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
My Web Search
Search
Address
http://localhost:100/scgi?sid=16b41157b4de7df915debacefd
Go
DesktopFun
Search
Screensavers
Games
Videos
eCards
Shopping
Links
Done
Local intranet

Server Account Settings > Server script execution

A script can be executed for specific server events. The event, account, connection IP and filenames are made available inside the script. Identical to Sysax FTP automation, the script can be used to send email, perform file transfer, local processing or run other programs.

☑ Enable server script execution based on connection events

☐ Execute script on successful login

☐ Execute script if login failed

☐ Execute script on file download completion

☐ Execute script on file upload completion

☐ Execute script after file deletion

☐ Execute script after file rename

Script path C:\Documents and Settings\user\Desktop\te [browse...]

[save] [Cancel]

9

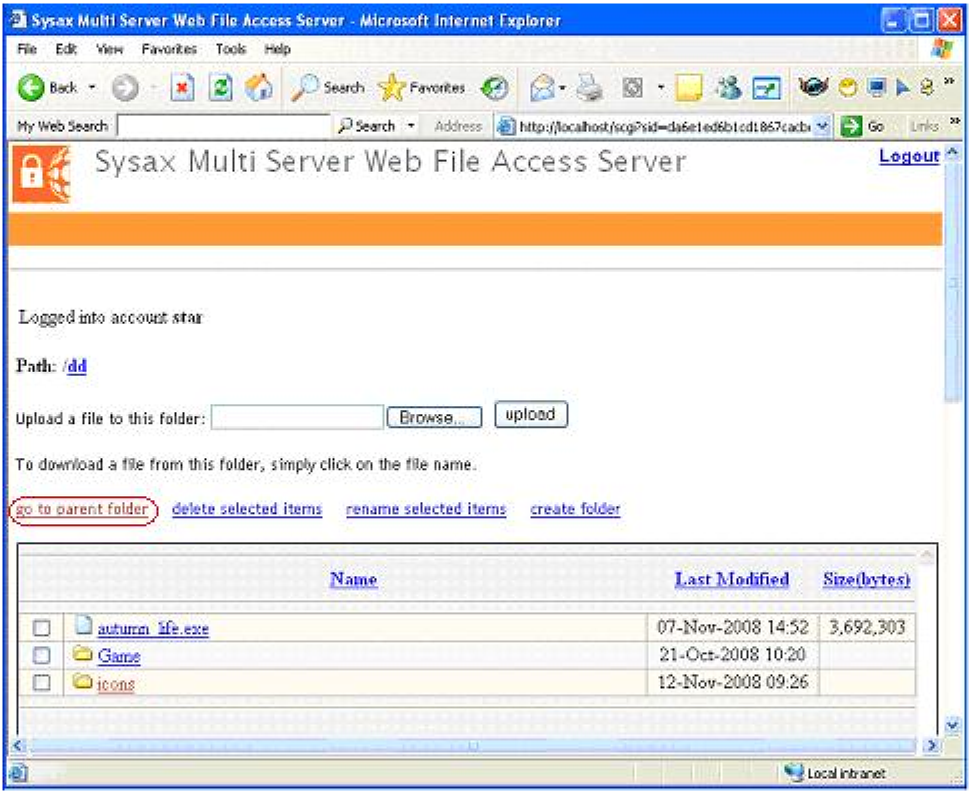
Using the Web File Access Interface

9.1. Links for Sysax Multi Server Web File Access Server Interface

The Web File Access server interface contains seven different links.
Go to parent folder link:

This link is used to go to the last working page visited from the current working page. Clicking this option shows the figure displayed below.

Figure 9.1. Go to Parent Folder Link


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
My Web Search Search Address http://localhost/scgi?sid=da6e1ed6b1cd1867cacb Go Links
Logout
Browse...
upload
go to parent folder
delete selected items
rename selected items
create folder
Local intranet

Sysax Multi Server Web File Access Server

Logged into account star

Path: /dd

Upload a file to this folder:

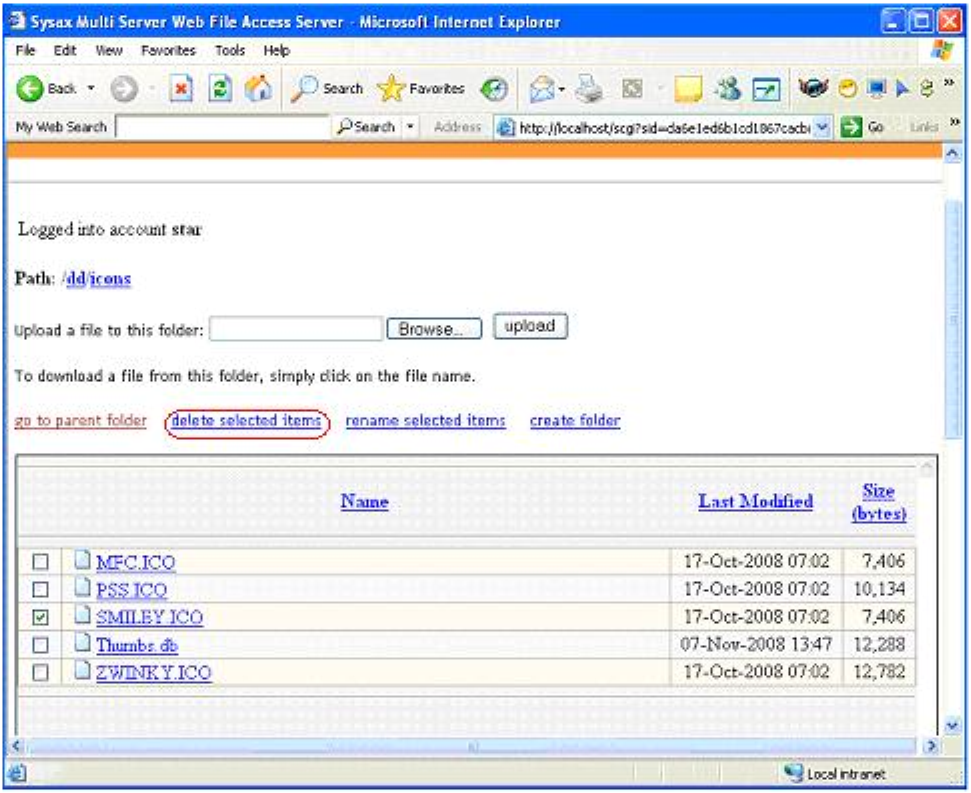
To download a file from this folder, simply click on the file name.

	Name	Last Modified	Size(bytes)
□	autumn_life.exe	07-Nov-2008 14:52	3,692,303
□	Game	21-Oct-2008 10:20	
□	icons	12-Nov-2008 09:26	

Delete selected items link:

The delete selected items link is used to delete the selected file or folder.

Figure 9.2. Delete Selected Items Link



Logged into account star

Path: /dd/icons

Upload a file to this folder:

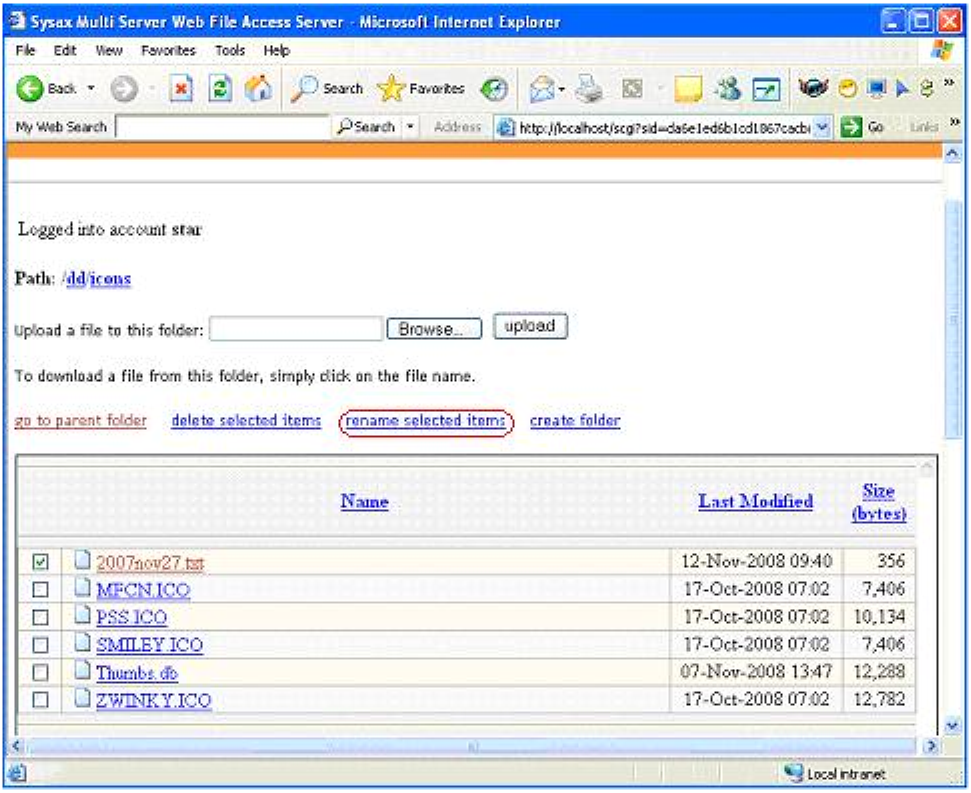
To download a file from this folder, simply click on the file name.

	Name	Last Modified	Size (bytes)
□	MFC.ICO	17-Oct-2008 07:02	7,406
□	PSS.ICO	17-Oct-2008 07:02	10,134
☑	SMILEY.ICO	17-Oct-2008 07:02	7,406
□	Thumbs.db	07-Nov-2008 13:47	12,288
□	ZWINKY.ICO	17-Oct-2008 07:02	12,782

Rename selected items link:

The rename selected items link is used to rename the selected file or folder.

Figure 9.3. Rename Selected Items Link


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
My Web Search Search Address http://localhost/scgi?sid=da6e1ed6b1cd1867cacb Go Links
Local intranet

Logged into account star

Path: /dd/icons

Upload a file to this folder: Browse... upload

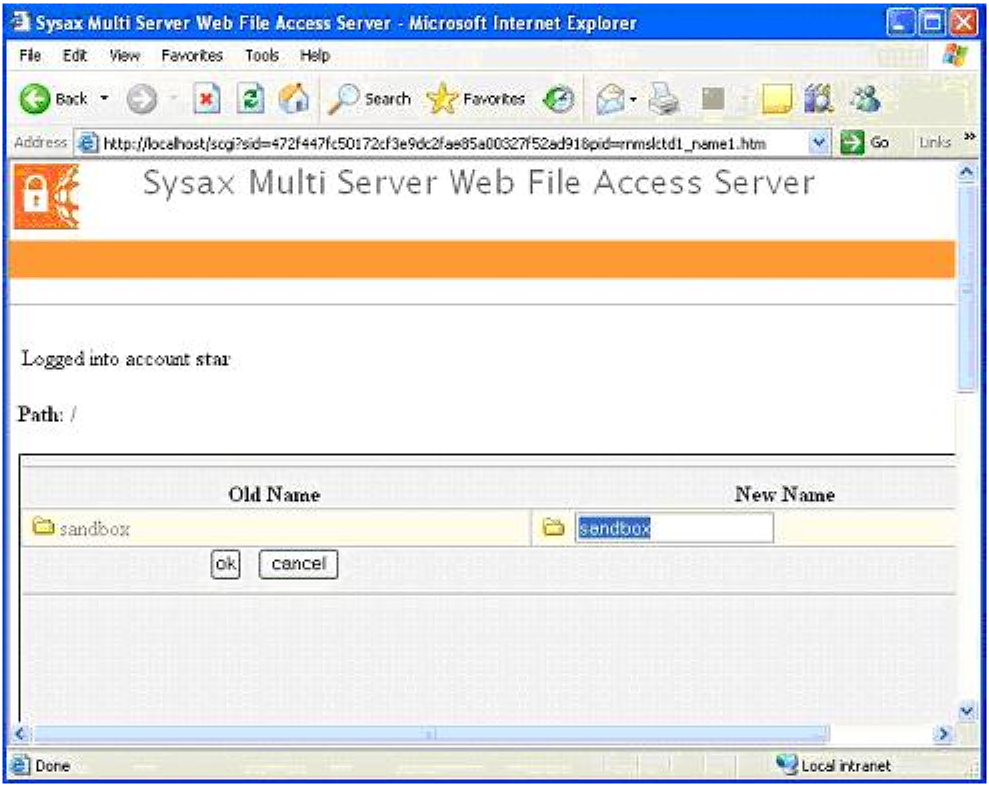
To download a file from this folder, simply click on the file name.

go to parent folder delete selected items rename selected items create folder

	Name	Last Modified	Size (bytes)
☑	2007nov27.txt	12-Nov-2008 09:40	356
□	MFCN.ICO	17-Oct-2008 07:02	7,406
□	PSS.ICO	17-Oct-2008 07:02	10,134
□	SMILEY.ICO	17-Oct-2008 07:02	7,406
□	Thumbs.db	07-Nov-2008 13:47	12,288
□	ZWINKY.ICO	17-Oct-2008 07:02	12,782

After clicking the rename selected items link, the following figure is displayed.

Figure 9.4. Renaming Selected Items


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://localhost/scgi?sid=472f447fc50172cf3e9dc2fae85a00327f52ad918pid=rnmslctd1_name1.htm
Go
Links
Sysax Multi Server Web File Access Server
ok
cancel
Done
Local intranet

Logged into account star

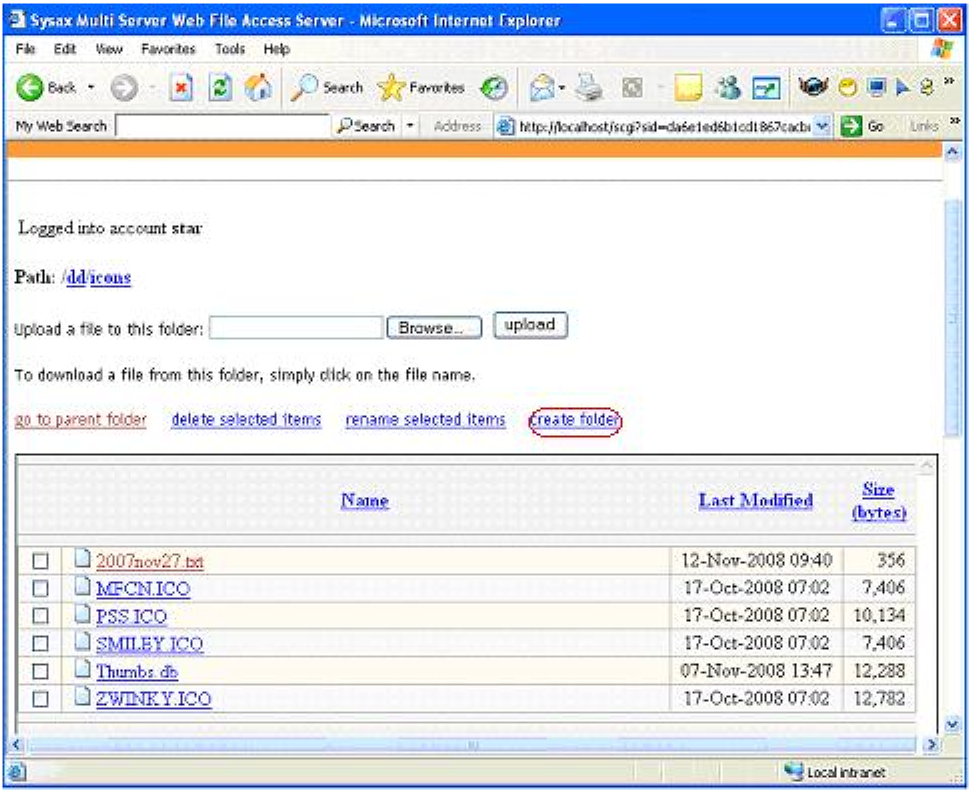
Path: /

Old Name	New Name
sandbox	sandbox

Create folder link:

The create folder link is used to create a folder into the selected path.

Figure 9.5. Create Folder Link


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
My Web Search
Search
Address
http://localhost/scgi?sid=da6e1ed6b1cd1867cacb
Go
Links
Browse...
upload
Local intranet

Logged into account star

Path: /dd/icons

Upload a file to this folder:

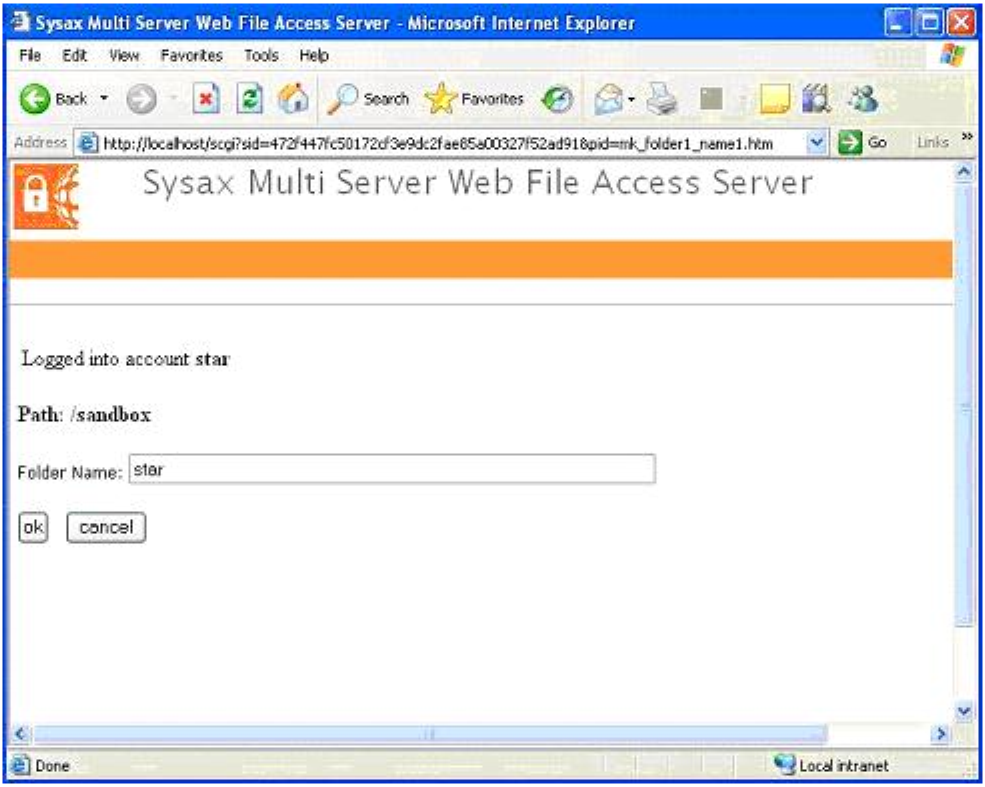
To download a file from this folder, simply click on the file name.

go to parent folder   delete selected items   rename selected items   create folder

	Name	Last Modified	Size (bytes)
□	2007nov27.txt	12-Nov-2008 09:40	356
□	MFCN.ICO	17-Oct-2008 07:02	7,406
□	PSS.ICO	17-Oct-2008 07:02	10,134
□	SMILEY.ICO	17-Oct-2008 07:02	7,406
□	Thumbs.db	07-Nov-2008 13:47	12,288
□	ZWINKY.ICO	17-Oct-2008 07:02	12,782

After clicking the create folder link, the following figure is displayed.

Figure 9.6. Creating a Folder



http://localhost/scgi?sid=472f447fc50172cf3e9dc2fae85a00327f52ad91&pid=mk_folder1_name1.htm

Sysax Multi Server Web File Access Server

Logged into account star

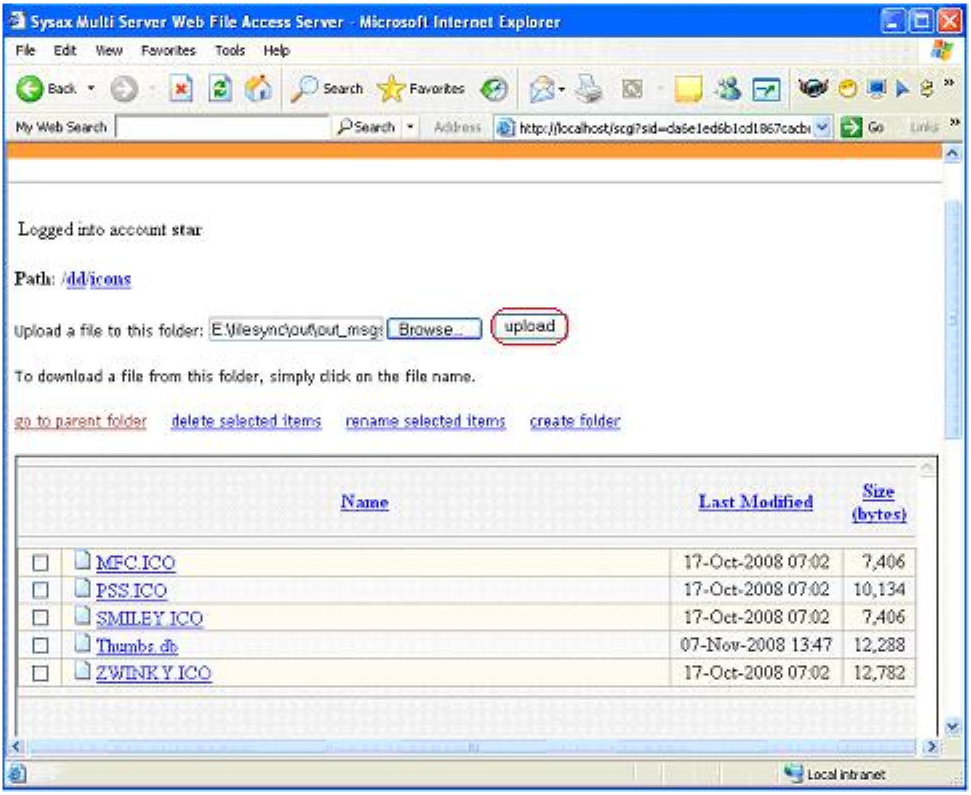
Path: /sandbox

Folder Name: star

Upload link:

The upload link is used to upload files. To upload a file, select the path from **upload the following file** field. Click the upload option (Figure 9.7).

Figure 9.7. Example of Upload Link


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
My Web Search Search Address
http://localhost/scgi?sid=da6e1ed6b1cd1867cacb
Go Links
Local intranet

Logged into account star

Path: /dd/icons

Upload a file to this folder: E:\filesync\out\out_msg: Browse... upload

To download a file from this folder, simply click on the file name.

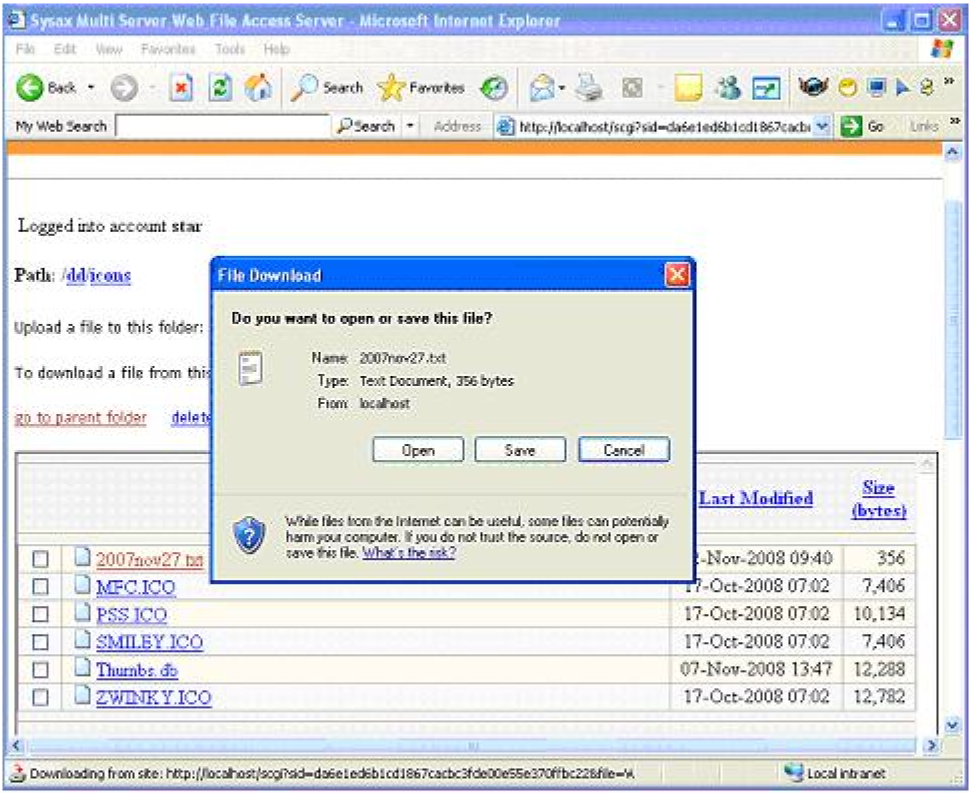
go to parent folder delete selected items rename selected items create folder

	Name	Last Modified	Size (bytes)
□	MFC.ICO	17-Oct-2008 07:02	7,406
□	PSS.ICO	17-Oct-2008 07:02	10,134
□	SMILEY.ICO	17-Oct-2008 07:02	7,406
□	Thumbs.db	07-Nov-2008 13:47	12,288
□	ZWINKY.ICO	17-Oct-2008 07:02	12,782

Download link:

If you want to download files, just double click the downloaded file from Web File Access Server Interface window. The **File Download** dialog box appears with the message: "Do you want to open or save this file?". Click the **save** button to download the file.

Figure 9.8. Example of Download Link


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
My Web Search Search Address http://localhost/scgi?sid=da6e1ed6b1cd1867cacb Go Links

Logged into account star

Path: /dd/icons

Upload a file to this folder:

To download a file from thi

go to parent folder delet

File Download

Do you want to open or save this file?

Name: 2007nov27.txt
Type: Text Document, 356 bytes
From: localhost

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

		Last Modified	Size (bytes)
□	2007nov27.txt	-Nov-2008 09:40	356
□	MFC.ICO	17-Oct-2008 07:02	7,406
□	PSS.ICO	17-Oct-2008 07:02	10,134
□	SMILEY.ICO	17-Oct-2008 07:02	7,406
□	Thumbs.db	07-Nov-2008 13:47	12,288
□	ZWINKY.ICO	17-Oct-2008 07:02	12,782

Downloading from site: http://localhost/scgi?sid=da6e1ed6b1cd1867cacbc3fde00e55e370ffbc22&file=\A

Logout

The logout button is used to logout the current working account.

10

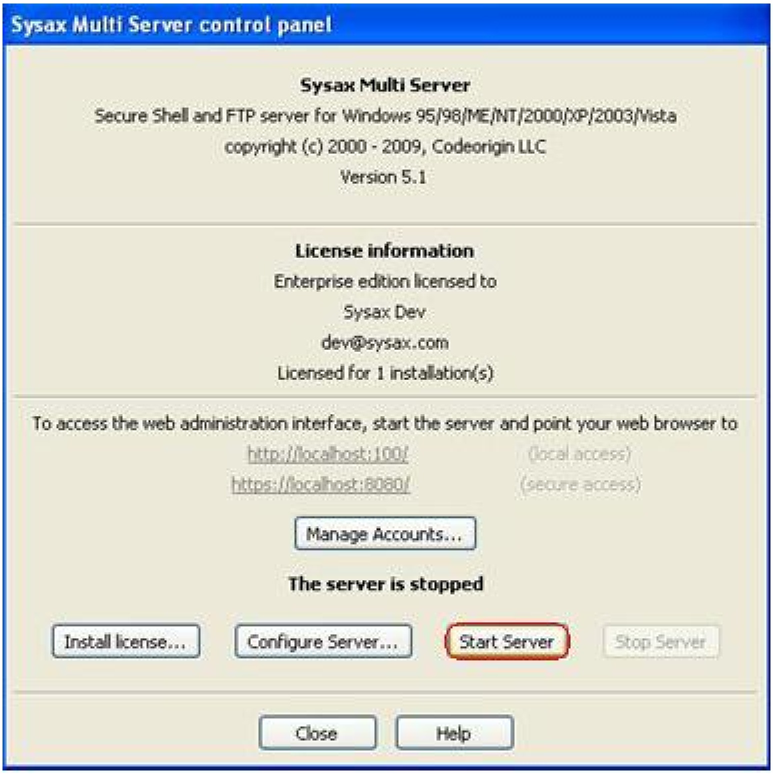
How to connect using FTP

Sysax Multi Server allows you to connect to the server in FTP, and to connect using the sysaxftp.exe file.

Connecting to Server

To connect to the server in FTP, go to the Sysax Multi Server control panel and click **Start Server**(See Figure 10.1).

Figure 10.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

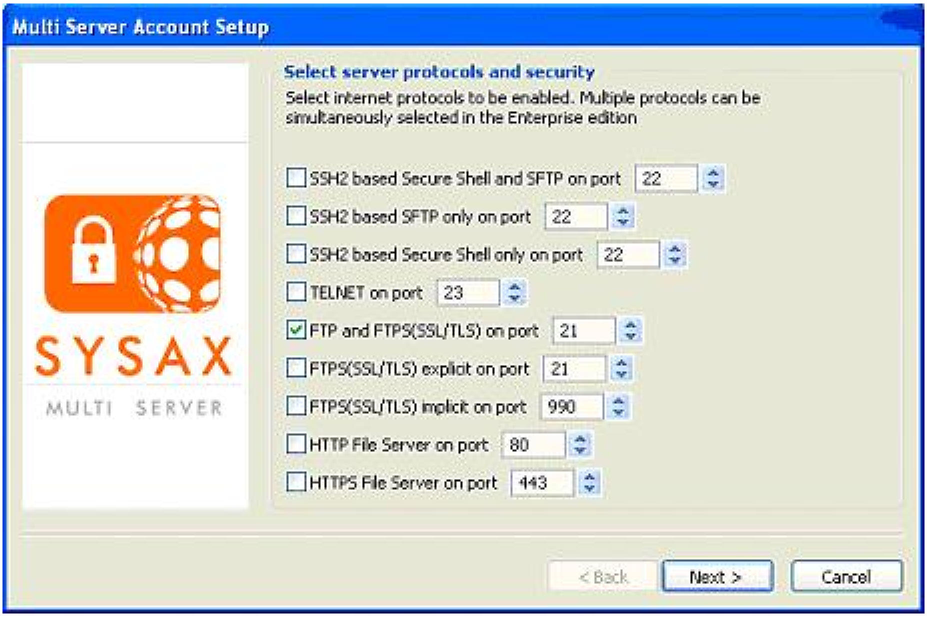
http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window appears(See Figure 10.2).

Figure 10.2. Connect Using FTP



Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

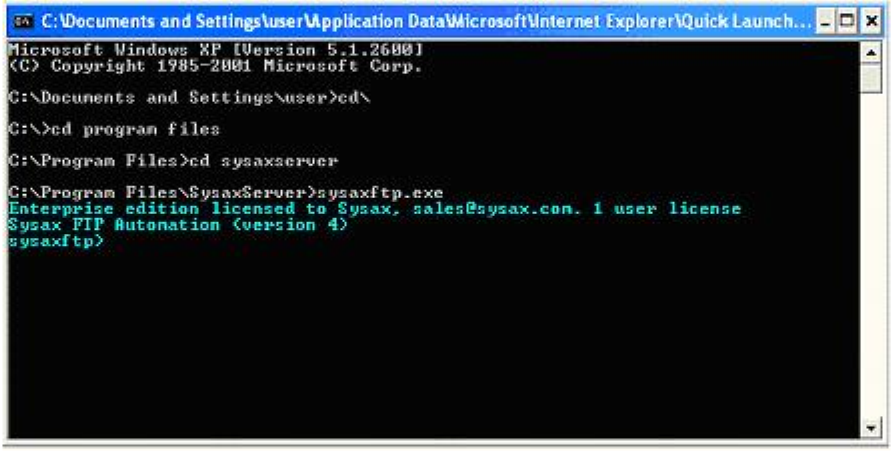
- □ SSH2 based Secure Shell and SFTP on port 22
- □ SSH2 based SFTP only on port 22
- □ SSH2 based Secure Shell only on port 22
- □ TELNET on port 23
- ☑ FTP and FTPS(SSL/TLS) on port 21
- □ FTPS(SSL/TLS) explicit on port 21
- □ FTPS(SSL/TLS) implicit on port 990
- □ HTTP File Server on port 80
- □ HTTPS File Server on port 443

Click **FTP and FTPS(SSL/TLS) on port**, set the port to **21**, and click **Next**.

Connecting to Server using sysaxftp.exe

To connect to the server using the sysaxftp.exe program, **double-click** the **sysaxftp.exe** icon, or run the **sysaxftp.exe** as shown below in Figure 10.3.

Figure 10.3. Windows Dos Command Window

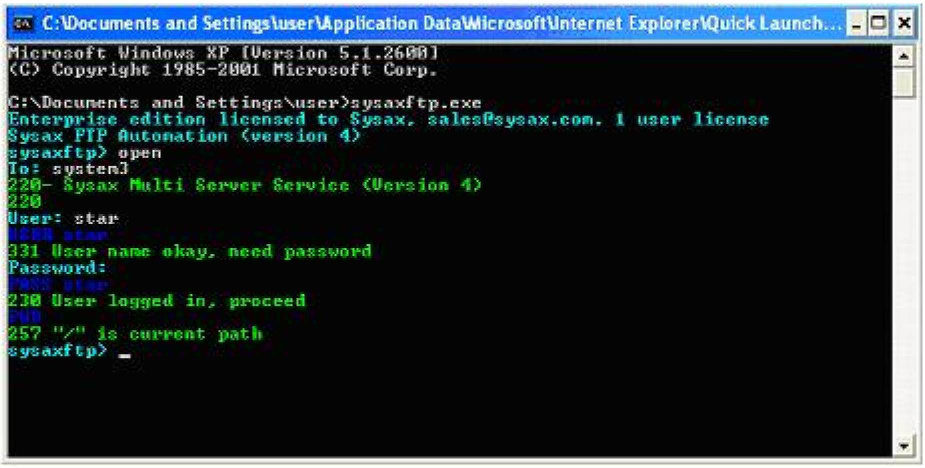

C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd\

C:\>cd program files

C:\Program Files>cd sysaxserver

C:\Program Files\SysaxServer>sysaxftp.exe
Enterprise edition licensed to Sysax, sales@sysax.com. 1 user license
Sysax FTP Automation (version 4)
sysaxftp>
```

Follow these steps to login the Sysaxftp session (Figure 10.4).

1. Enter the **open** command.
2. Enter the **host name(IP address)**.
3. Enter **user name** and **password**.

Figure 10.4. Sysaxftp Dos Command Window


C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>sysaxftp.exe
Enterprise edition licensed to Sysax, sales@sysax.com. 1 user license
Sysax FTP Automation (version 4)
sysaxftp> open
To: system3
220- Sysax Multi Server Service (Version 4)
220
User: star
USER star
331 User name okay, need password
Password:
PASS star
230 User logged in, proceed
PWD
257 "/" is current path
sysaxftp> _
```

11

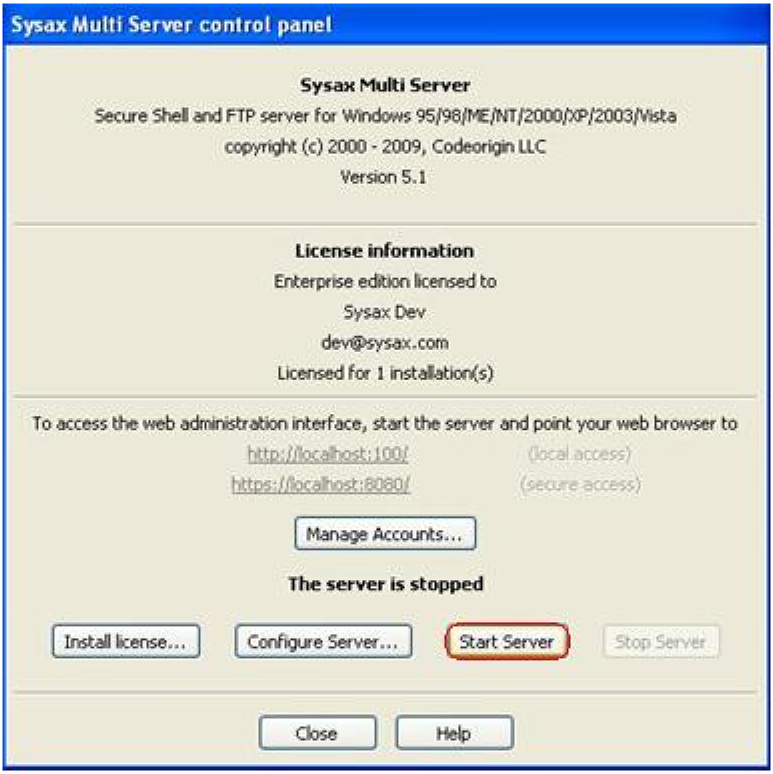
How to connect using FTPS

Sysax Multi Server allows you to connect to the server in FTPS, and to connect using the sysaxftp.exe file.

Connecting to Server

To connect to the server in FTPS(SSL/TLS) explicit, go to the Sysax Multi Server control panel and click **Start Server**(See Figure 11.1).

Figure 11.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server
Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista
copyright (c) 2000 - 2009, Codeorigin LLC
Version 5.1

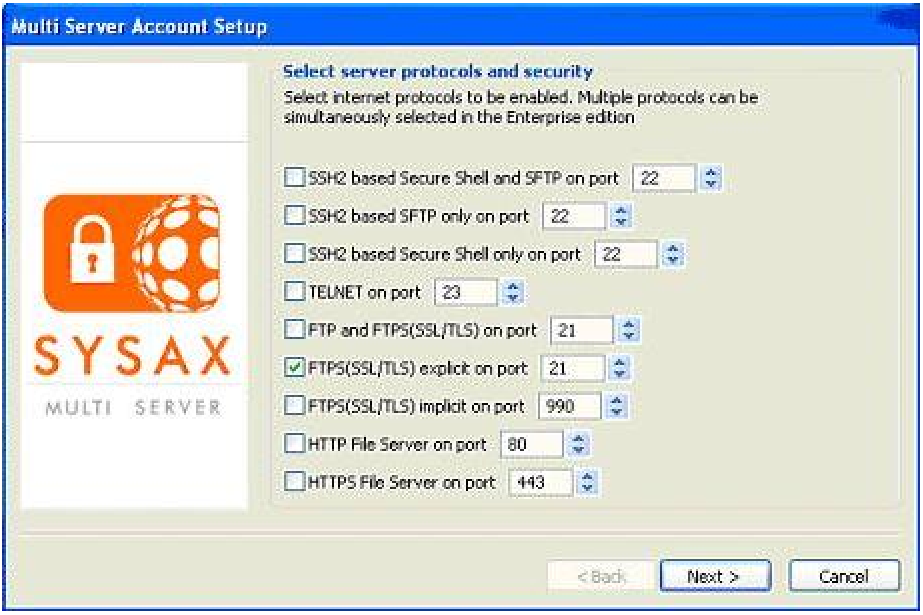
License information
Enterprise edition licensed to
Sysax Dev
dev@sysax.com
Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to
http://localhost:100/ (local access)
https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window appears(See Figure 11.2).

Figure 11.2. Connect Using FTPS(SSL/TLS) Explicit



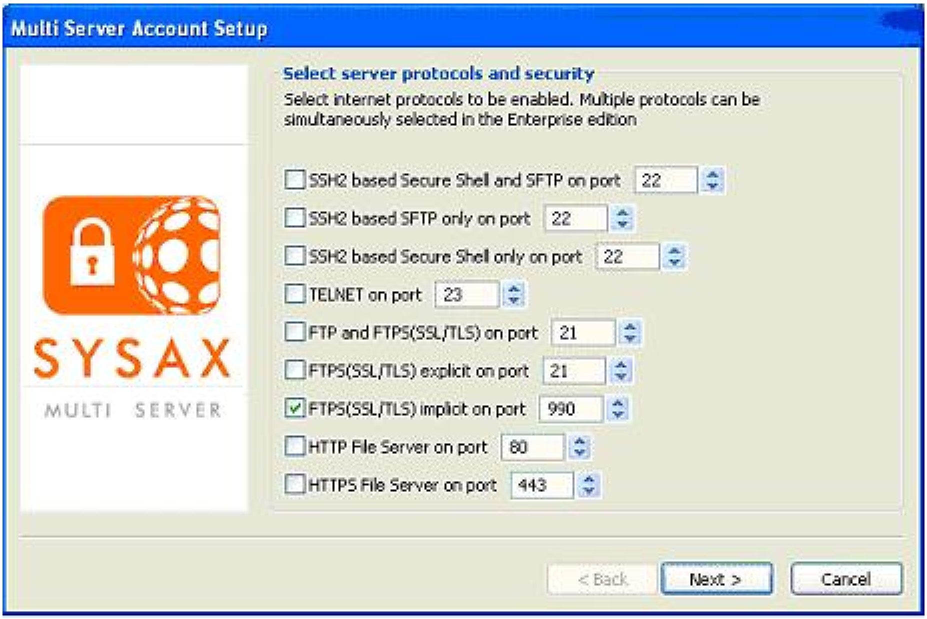
Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

- ☐ SSH2 based Secure Shell and SFTP on port 22
- ☐ SSH2 based SFTP only on port 22
- ☐ SSH2 based Secure Shell only on port 22
- ☐ TELNET on port 23
- ☐ FTP and FTPS(SSL/TLS) on port 21
- ☑ FTPS(SSL/TLS) explicit on port 21
- ☐ FTPS(SSL/TLS) implicit on port 990
- ☐ HTTP File Server on port 80
- ☐ HTTPS File Server on port 443

To connect to the server in FTPS(SSL/TLS) implicit, the multi-server account setup window appears(See Figure 11.3).

Figure 11.3. Connect using FTPS(SSL/TLS) implicit



Multi Server Account Setup

Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

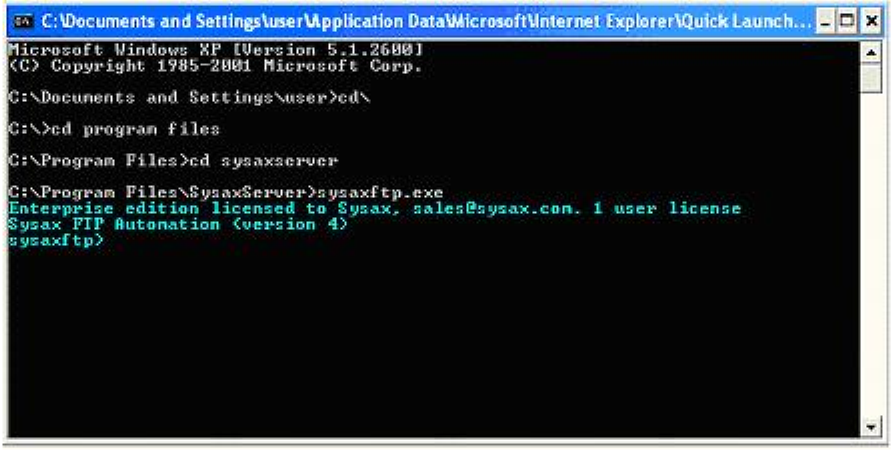
- □ SSH2 based Secure Shell and SFTP on port 22
- □ SSH2 based SFTP only on port 22
- □ SSH2 based Secure Shell only on port 22
- □ TELNET on port 23
- □ FTP and FTPS(SSL/TLS) on port 21
- □ FTPS(SSL/TLS) explicit on port 21
- ☑ FTPS(SSL/TLS) implicit on port 990
- □ HTTP File Server on port 80
- □ HTTPS File Server on port 443

Click for the **FTPS(SSL/TLS) explicit on port**, set the port to **21** and **FTPS(SSL/TLS) implicit on port**, set the port to **990**, and click **Next**.

Connecting to Server using sysaxftp.exe

To connect to the server using the sysaxftp.exe program, double-click the sysaxftp.exe icon, or run the sysaxftp.exe as shown below in Figure 11.4.

Figure 11.4. Windows Dos Command Window



C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd\

C:\>cd program files

C:\Program Files>cd sysaxserver

C:\Program Files\SysaxServer>sysaxftp.exe
Enterprise edition licensed to Sysax, sales@sysax.com. 1 user license
Sysax FTP Automation (version 4)
sysaxftp>
```

Follow these steps to login the Sysaxftp session for both FTPS(SSL/TLS) explicit and FTPS(SSL/TLS) implicit protocols.

1. Enter the **ssl** protocol option.

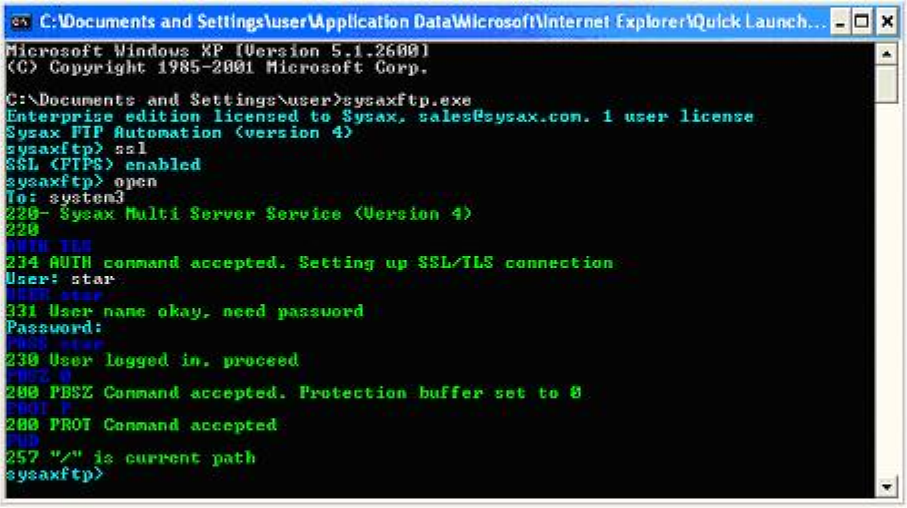
2. Enter the **open** command.

3. Enter the **host name(IP address)**.

4. Enter **user name** and **password**.

The Sysaxftp window is displayed(See Figure 11.5).

Figure 11.5. Sysaxftp Dos Command Window



C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>sysaxftp.exe
Enterprise edition licensed to Sysax, sales@sysax.com. 1 user license
Sysax FTP Automation (version 4)
sysaxftp> ssl
SSL (FTPS) enabled
sysaxftp> open
To: system3
220- Sysax Multi Server Service (Version 4)
220
AUTH TLS
234 AUTH command accepted. Setting up SSL/TLS connection
User: star
USER star
331 User name okay, need password
Password:
PASS star
230 User logged in, proceed
PBSZ 0
200 PBSZ Command accepted. Protection buffer set to 0
PROT P
200 PROT Command accepted
PWD
257 "/" is current path
sysaxftp>
```

12

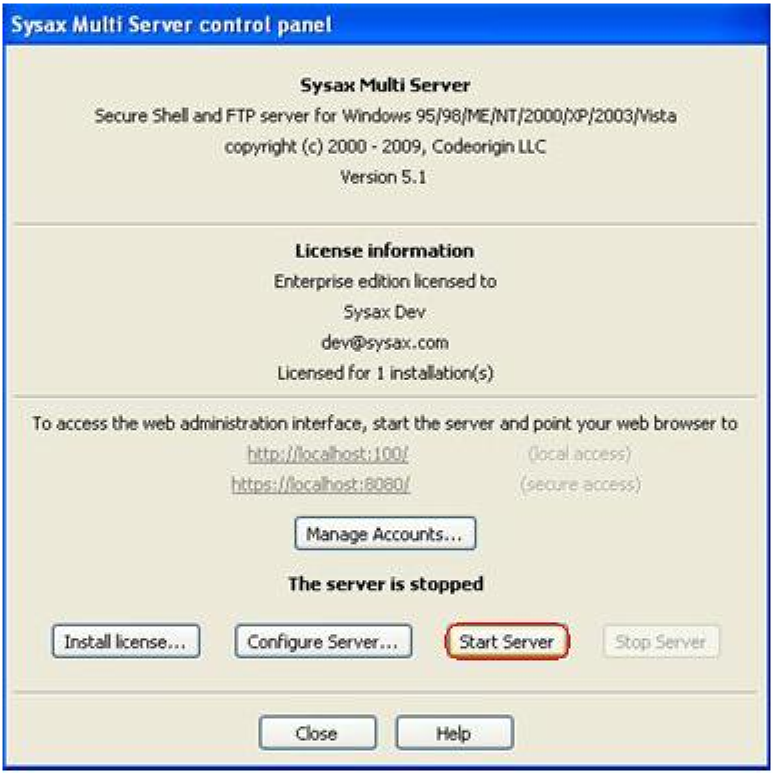
How to Connect Using Telnet

Sysax Multi Server enables you to connect to the server using a Telnet-only shell interface.

Connecting to Server

To connect to the server using a Telnet-only shell interface, go to the Sysax Multi Server control panel and click Start Server(Figure 12.1)

Figure 12.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

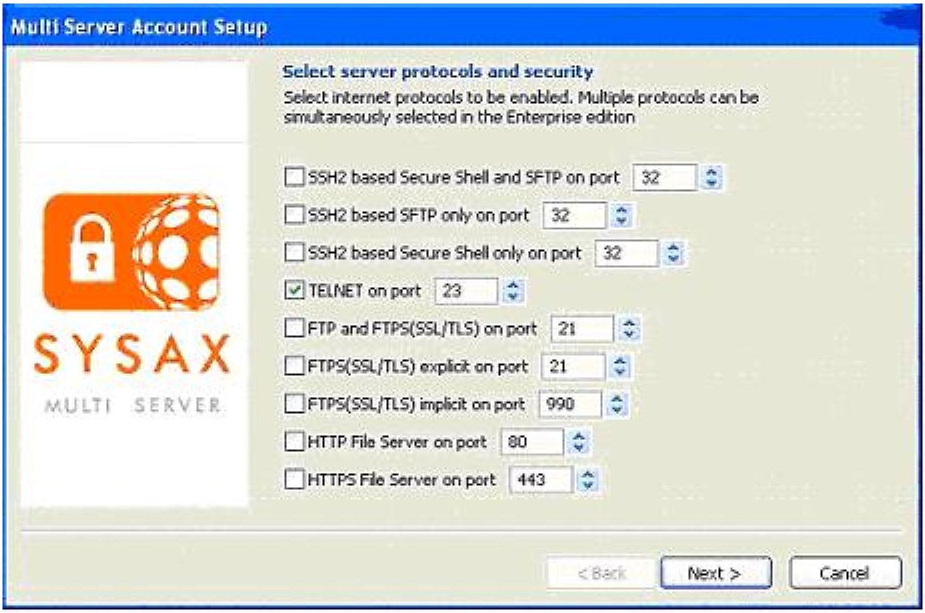
http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window is displayed(Figure 12.2).

Figure 12.2. Connect Using Telnet



Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

□ SSH2 based Secure Shell and SFTP on port 32

□ SSH2 based SFTP only on port 32

□ SSH2 based Secure Shell only on port 32

☑ TELNET on port 23

□ FTP and FTPS(SSL/TLS) on port 21

□ FTPS(SSL/TLS) explicit on port 21

□ FTPS(SSL/TLS) implicit on port 990

□ HTTP File Server on port 80

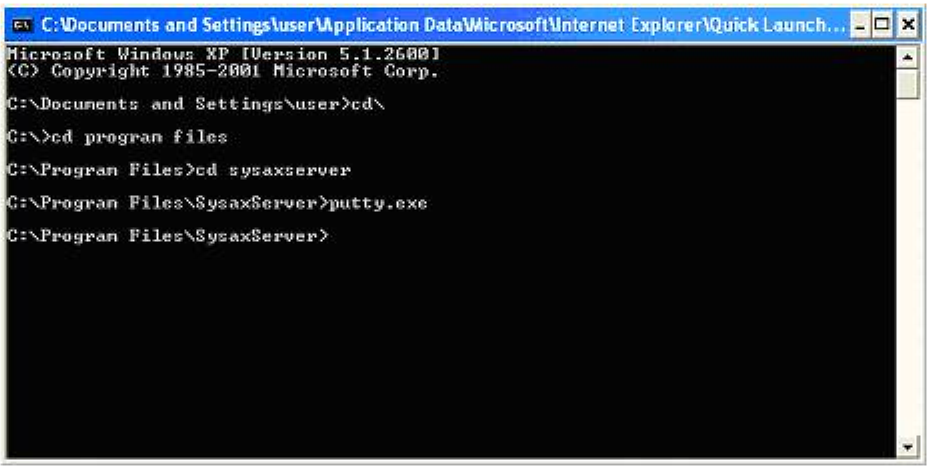
□ HTTPS File Server on port 443

Click **Telnet on port**, set the port to **23**, and click **Next**.

Connecting to Server Using PuTTY.exe

To connect to the server using the putty.exe program, double-click the putty.exe icon, or run the putty.exe command as shown below in Figure 12.3.

Figure 12.3. Windows Dos Command Window

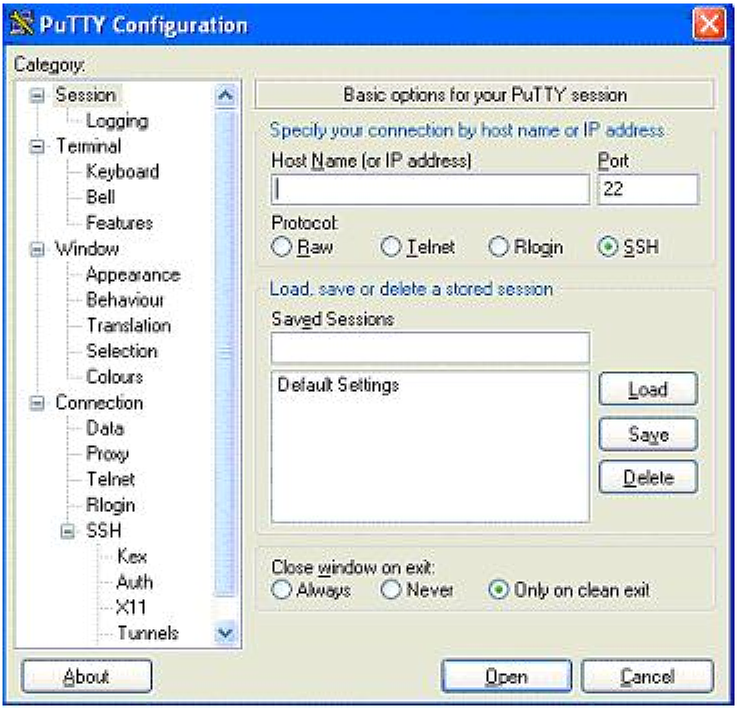

C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd\

C:\>cd program files

C:\Program Files>cd sysaxserver

C:\Program Files\SysaxServer>putty.exe

C:\Program Files\SysaxServer>
```

Configuring PuTTy.exe

The PuTTY Configuration screen is displayed(Figure 12.4).

Figure 12.4. PuTTY Configuration



Host Name (or IP address)

Port 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Connecting in Telnet-only Interface

Follow these steps to configure the PuTTY session.

1. Enter the host name(IP address).

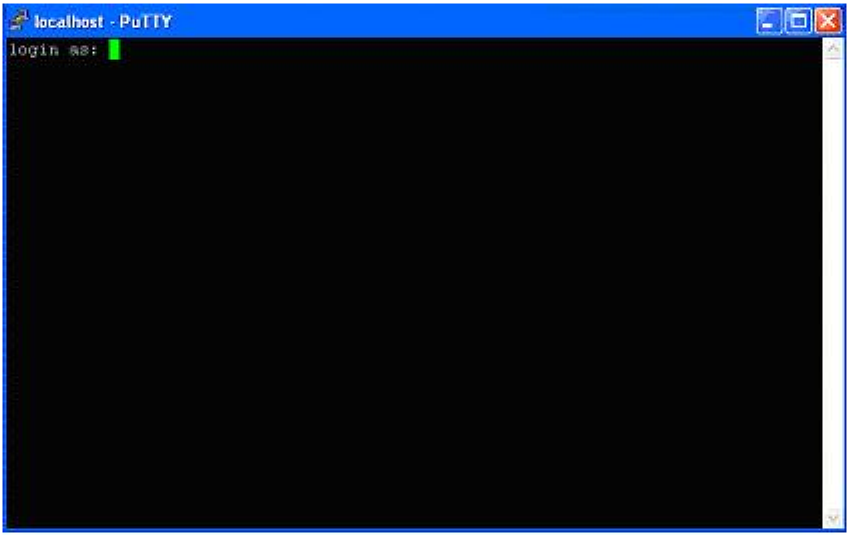
2. Select **Telnet** protocol.

3. Enter **23** in the **Port** field.

4. Click **Open**.

The **PuTTY** window is displayed(See Figure 12.5)

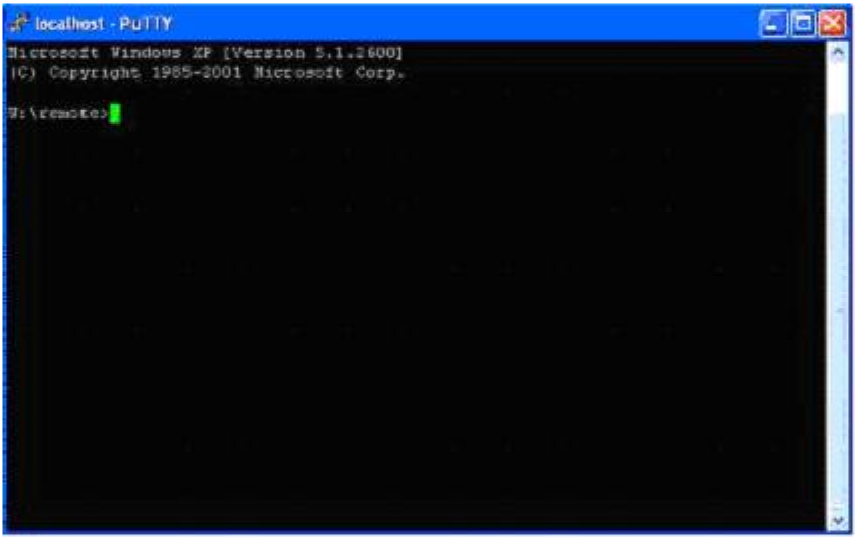
Figure 12.5. PuTTY Command Line



```
login as:
```

At the log-in command line, enter the login name and password to open the protected FTP account or Windows user account(Figure 13.6).

Figure 12.6. PuTTY system Command Line



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\remote>
```

13

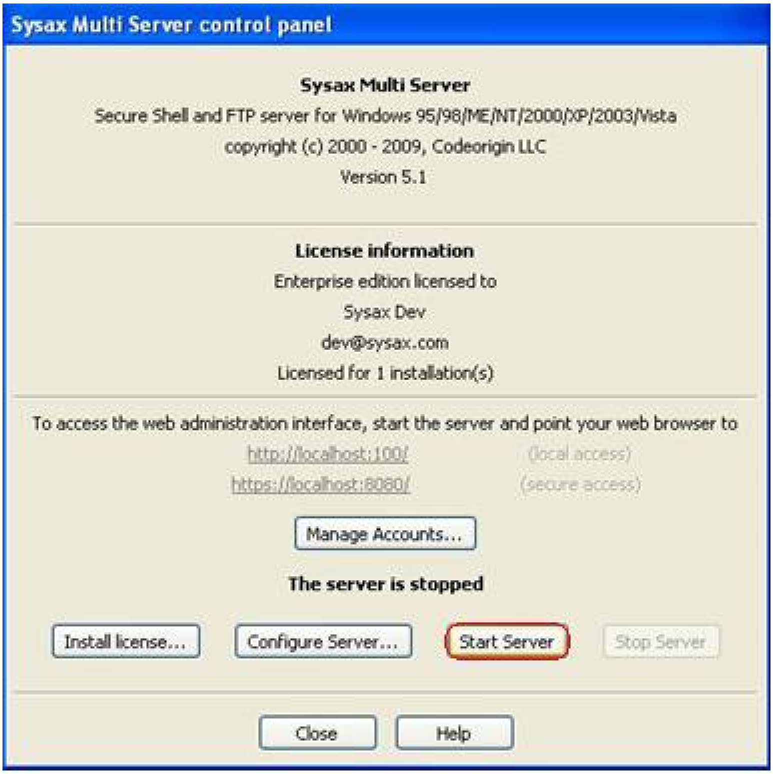
How to Connect Using SFTP

Sysax Multi Server allows you to connect to the server in SFTP, and to connect using the sysaxftp.exe file.

Connecting to Server

To connect to the server in SSH2 based Secure Shell and SFTP, go to the Sysax Multi Server control panel and click Start Server(Figure 13.1).

Figure 13.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

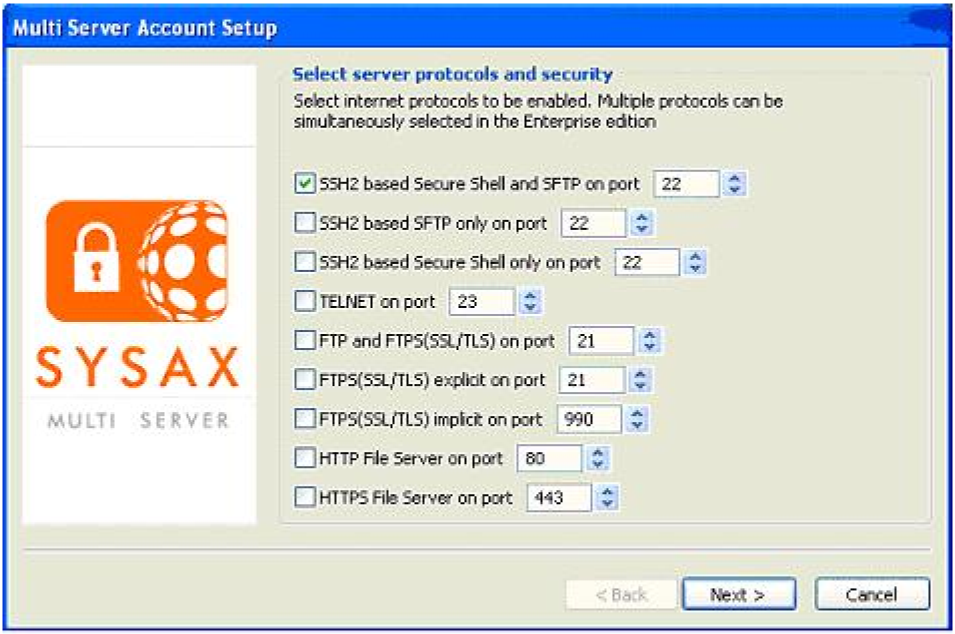
http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window appears(Figure 13.2).

Figure 13.2. Connect Using SSH2 based Secure Shell and SFTP



Multi Server Account Setup

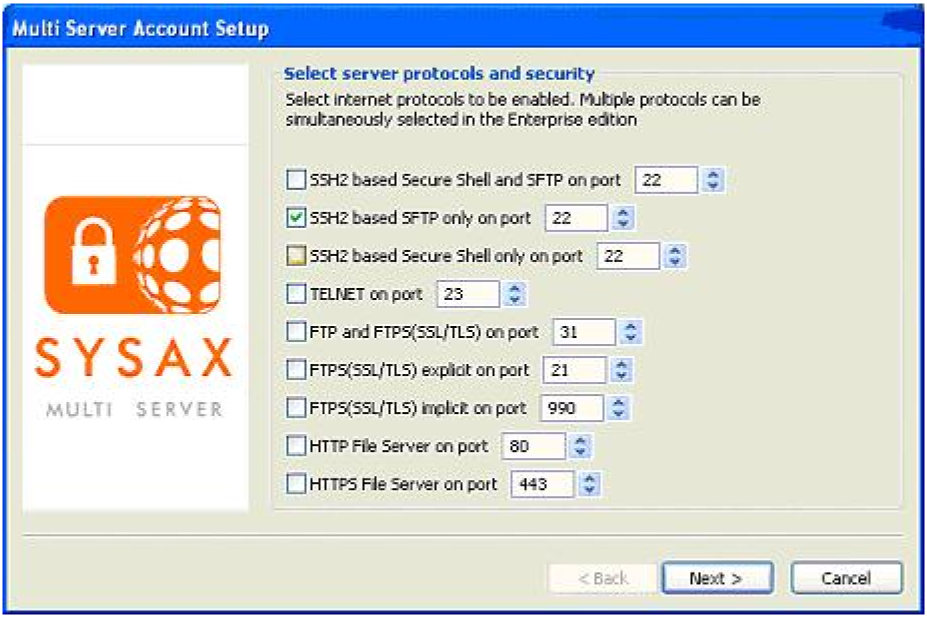
Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

- ☑ SSH2 based Secure Shell and SFTP on port 22
- □ SSH2 based SFTP only on port 22
- □ SSH2 based Secure Shell only on port 22
- □ TELNET on port 23
- □ FTP and FTPS(SSL/TLS) on port 21
- □ FTPS(SSL/TLS) explicit on port 21
- □ FTPS(SSL/TLS) implicit on port 990
- □ HTTP File Server on port 80
- □ HTTPS File Server on port 443

To connect to the server in SSH2 based SFTP, the multi-server account setup window appears(Figure 13.3).

Figure 13.3. Connect using SSH2 Based SFTP



Multi Server Account Setup

Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

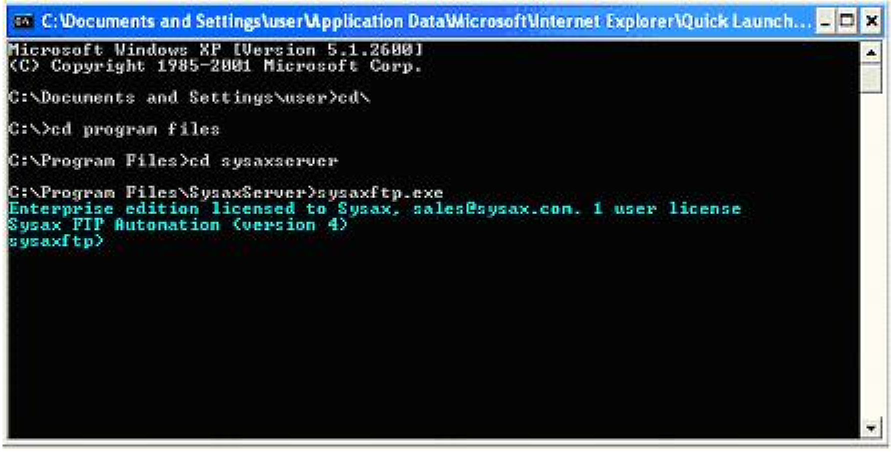
- □ SSH2 based Secure Shell and SFTP on port 22
- ☑ SSH2 based SFTP only on port 22
- □ SSH2 based Secure Shell only on port 22
- □ TELNET on port 23
- □ FTP and FTPS(SSL/TLS) on port 31
- □ FTPS(SSL/TLS) explicit on port 21
- □ FTPS(SSL/TLS) implicit on port 990
- □ HTTP File Server on port 80
- □ HTTPS File Server on port 443

Click both **SSH2 based Secure Shell** and **SFTP and SSH2 based SFTP on port**, set the port to **22**, and click **Next**.

Connecting to Server using sysaxftp.exe

To connect to the server using the sysaxftp.exe program, double-click the **sysaxftp.exe** icon, or run the sysaxftp.exe as shown below in Figure 13.4.

Figure 13.4. Windows Dos Command Window



C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

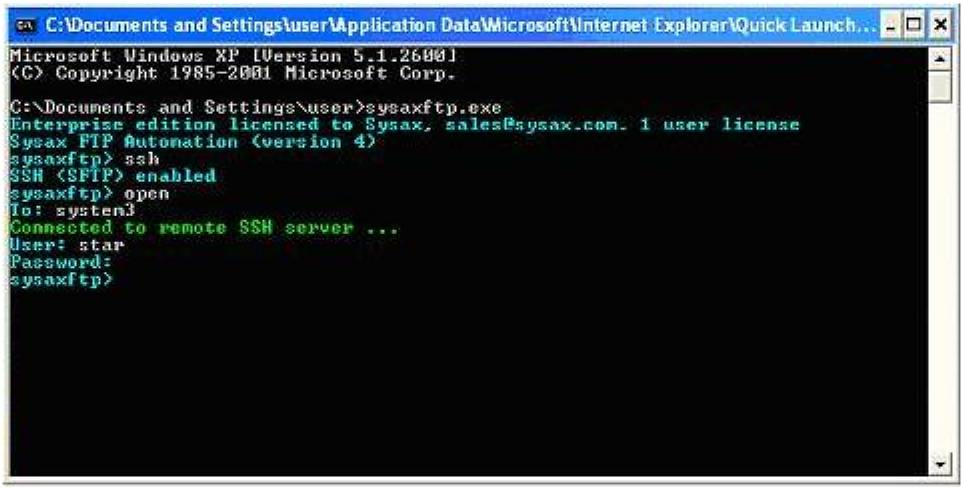
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd\

C:\>cd program files

C:\Program Files>cd sysaxserver

C:\Program Files\SysaxServer>sysaxftp.exe
Enterprise edition licensed to Sysax, sales@sysax.com. 1 user license
Sysax FTP Automation (version 4)
sysaxftp>
```

Follow these steps to login the Sysaxftp session.

1. Enter the **ssh** protocol option.
2. Enter the **open** command.
3. Enter the **host name(IP address)**.
4. Enter **user name** and **password**.

The Sysaxftp window is displayed(Figure 13.5).

Figure 13.5. Sysaxftp Dos Command Window



C:\Documents and Settings\user\Application Data\Microsoft\Internet Explorer\Quick Launch...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>sysaxftp.exe
Enterprise edition licensed to Sysax, sales@sysax.com. 1 user license
Sysax FTP Automation (version 4)
sysaxftp> ssh
SSH (SFTP) enabled
sysaxftp> open
To: system3
Connected to remote SSH server ...
User: star
Password:
sysaxftp>
```

14

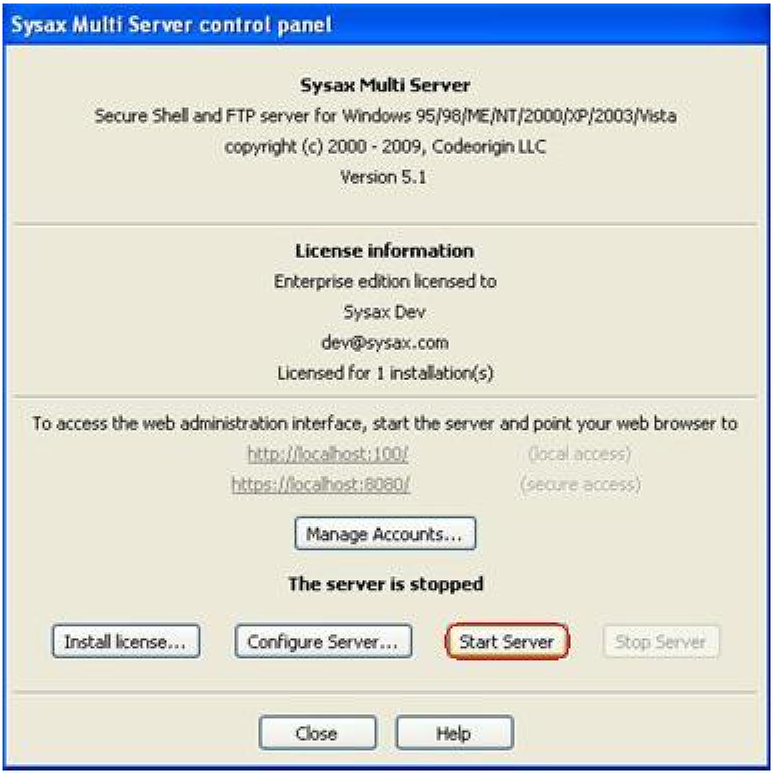
How to Connect Using SSH2 Secure Shell

Sysax Multi Server allows you to connect to the server in an SSH-only shell interface, and to connect using the PuTTy.exe file (See Chapter 12).

Connecting to Server

To connect to the server in an SSH-only shell interface, go to the Sysax Multi Server control Panel and click Start Server(See Figure 14.1).

Figure 14.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server

Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista

copyright (c) 2000 - 2009, Codeorigin LLC

Version 5.1

License information

Enterprise edition licensed to

Sysax Dev

dev@sysax.com

Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to

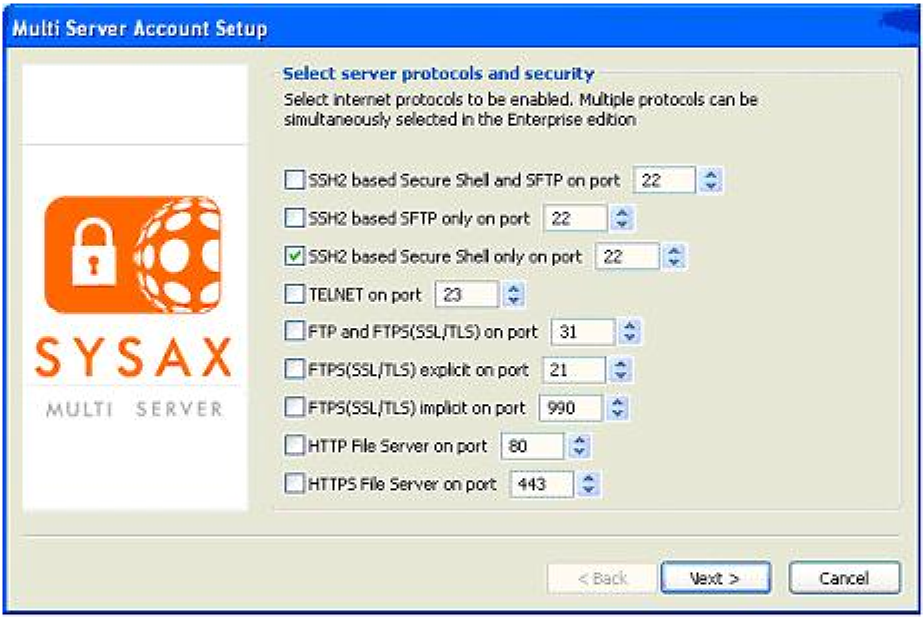
http://localhost:100/ (local access)

https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window appears(Figure 14.2).

Figure 14.2. Connect Using SSH2 Based Secure Shell Only



Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

- □ SSH2 based Secure Shell and SFTP on port 22
- □ SSH2 based SFTP only on port 22
- ☑ SSH2 based Secure Shell only on port 22
- □ TELNET on port 23
- □ FTP and FTPS(SSL/TLS) on port 31
- □ FTPS(SSL/TLS) explicit on port 21
- □ FTPS(SSL/TLS) implicit on port 990
- □ HTTP File Server on port 80
- □ HTTPS File Server on port 443

Click **SSH2 based Secure Shell only on port**, set the port to **22**, and click **Next**.

15

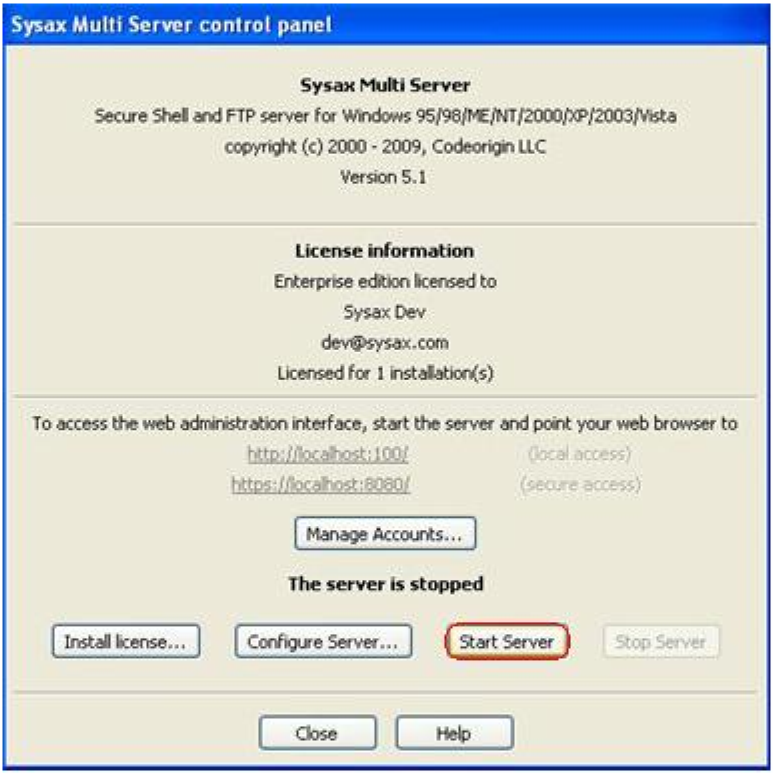
How to Connect Using HTTP

Sysax Multi Server allows you to connect to the server in **HTTP** interface, and to connect using the **web browser**.

Connecting to Server

To connect to the server in HTTP, go to the Sysax Multi Server control Panel and click Start Server (Figure 15.1).

Figure 15.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server
Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista
copyright (c) 2000 - 2009, Codeorigin LLC
Version 5.1

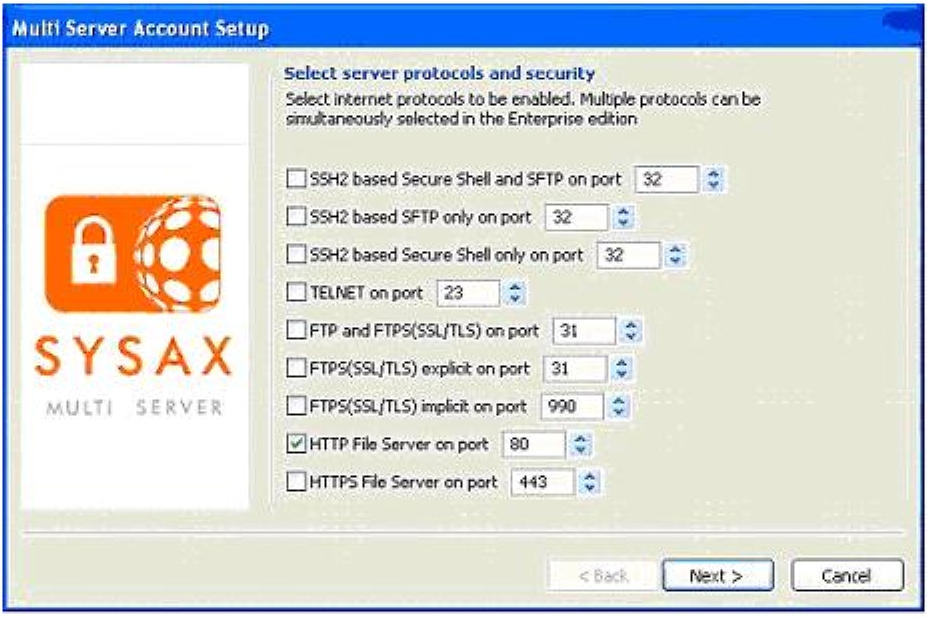
License information
Enterprise edition licensed to
Sysax Dev
dev@sysax.com
Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to
http://localhost:100/ (local access)
https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window appears(See Figure 15.2).

Figure 15.2. Connect Using HTTP



Multi Server Account Setup

Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

- □ SSH2 based Secure Shell and SFTP on port 32
- □ SSH2 based SFTP only on port 32
- □ SSH2 based Secure Shell only on port 32
- □ TELNET on port 23
- □ FTP and FTPS(SSL/TLS) on port 31
- □ FTPS(SSL/TLS) explicit on port 31
- □ FTPS(SSL/TLS) implicit on port 990
- ☑ HTTP File Server on port 80
- □ HTTPS File Server on port 443

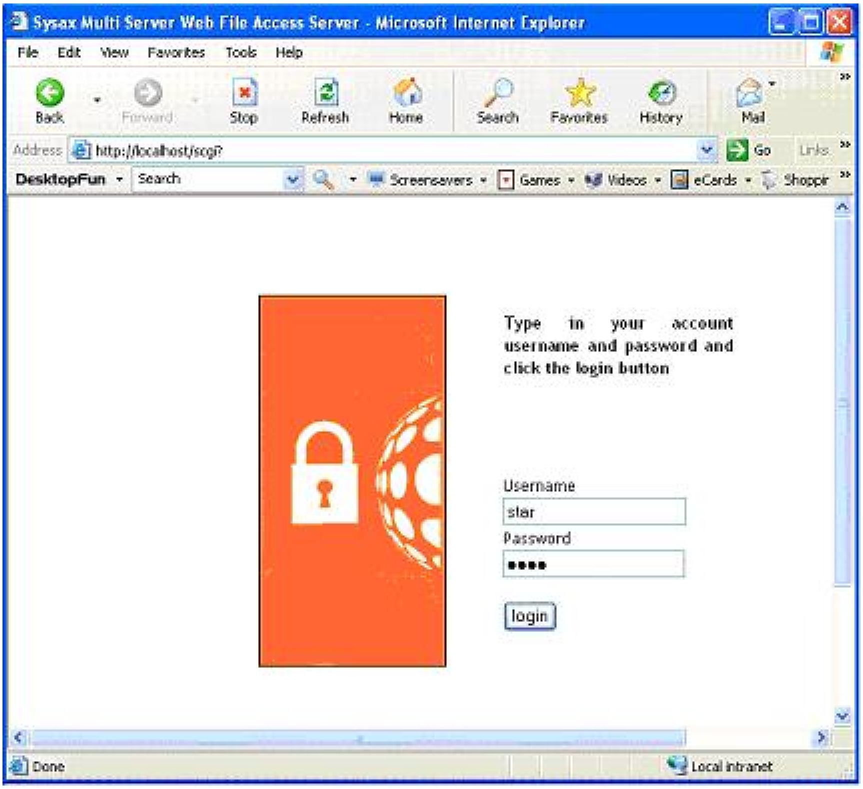
Click **HTTP File Server on port**, set the port to **80**, and click **Next**.

Connecting to Server Using Web Browser

To connect to the server using the web browser, double-click the internet explorer icon, then enter the local host address and select the Click to Login button. Enter the user name and password to login the web file access server.

The login page of Sysax Multi Server Web File Access Server is displayed(Figure 15.3).

Figure 15.3. Login the Sysax Multi Server Web File Access Server

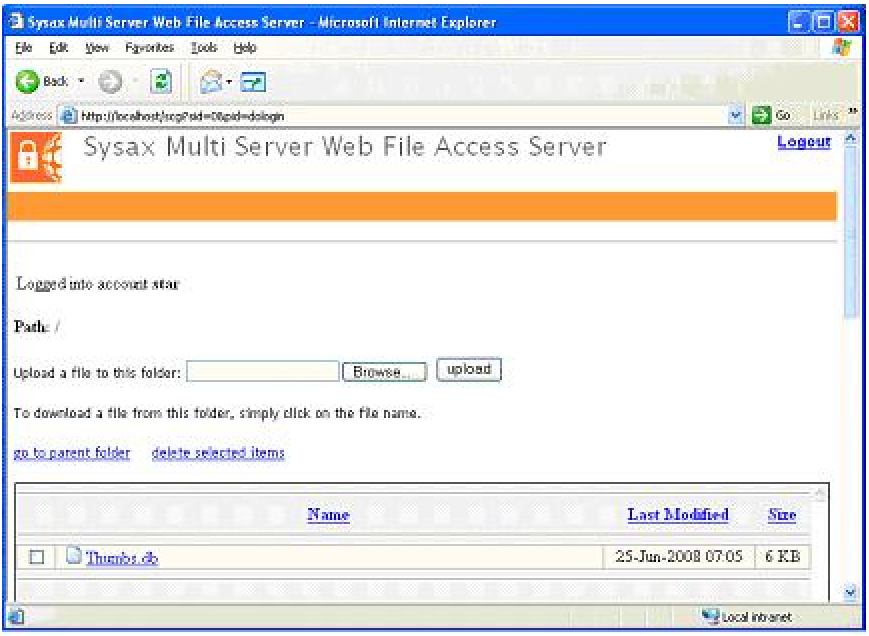

Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail
Address http://localhost/scgi?
Go Links
DesktopFun Search Screensavers Games Videos eCards Shoppir
Done
Local intranet

Type in your account username and password and click the login button

Username
star
Password
●●●●
login

The opened Sysax Multi Server Web File Access Server is shown in Figure 15.4.

Figure 15.4. Sysax Multi Server Web File Access Server


Sysax Multi Server Web File Access Server - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Address
http://localhost/scgi?sid=0&pid=dologin
Go
Links
Sysax Multi Server Web File Access Server
Logout
Browse...
upload
go to parent folder
delete selected items
Local intranet

Logged into account star

Path: /

Upload a file to this folder:

To download a file from this folder, simply click on the file name.

	Name	Last Modified	Size
□	Thumbs.db	25-Jun-2008 07:05	6 KB

16

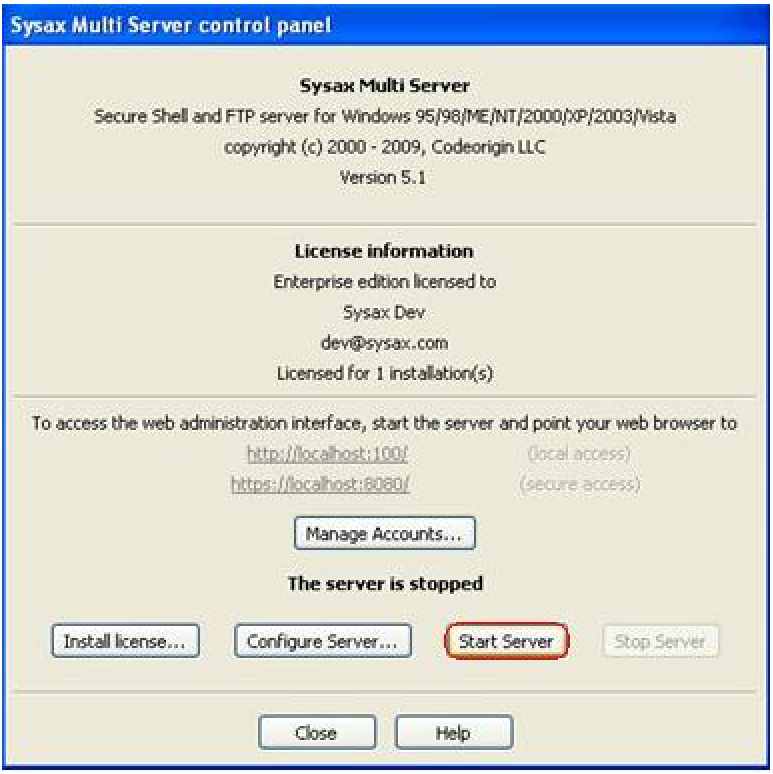
How to Connect Using HTTPS

Sysax Multi Server allows you to connect to the server in HTTPS interface, and to connect using the web browser.

Connecting to Server

To connect to the server in HTTPS, go to the Sysax Multi Server control Panel and click Start Server(Figure 16.1).

Figure 16.1. Start Server



Sysax Multi Server control panel

Sysax Multi Server
Secure Shell and FTP server for Windows 95/98/ME/NT/2000/XP/2003/Vista
copyright (c) 2000 - 2009, Codeorigin LLC
Version 5.1

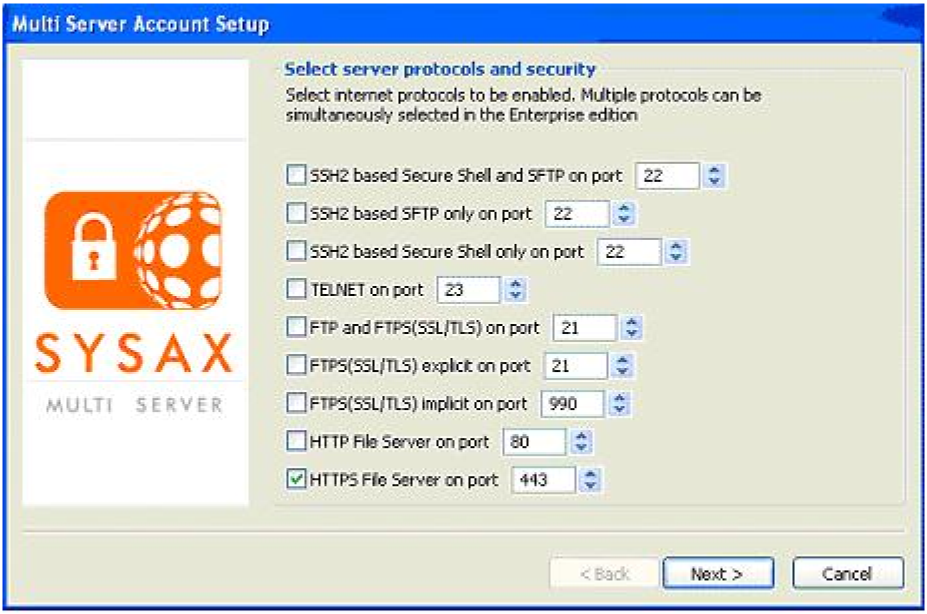
License information
Enterprise edition licensed to
Sysax Dev
dev@sysax.com
Licensed for 1 installation(s)

To access the web administration interface, start the server and point your web browser to
http://localhost:100/ (local access)
https://localhost:8080/ (secure access)

The server is stopped

The multi-server account setup window appears(Figure 16.2).

Figure 16.2. Connect Using HTTPS



Multi Server Account Setup

Select server protocols and security

Select internet protocols to be enabled. Multiple protocols can be simultaneously selected in the Enterprise edition

☐ SSH2 based Secure Shell and SFTP on port 22

☐ SSH2 based SFTP only on port 22

☐ SSH2 based Secure Shell only on port 22

☐ TELNET on port 23

☐ FTP and FTPS(SSL/TLS) on port 21

☐ FTPS(SSL/TLS) explicit on port 21

☐ FTPS(SSL/TLS) implicit on port 990

☐ HTTP File Server on port 80

☑ HTTPS File Server on port 443

Click **HTTPS File Server on port**, set the port to **443**, and click **Next**.

Connecting to Server Using Web Browser

To connect to the server using the web browser, and double-click the internet explorer icon. Then enter the local host address and select the Click to Login button. After entering the user name and password, login to the SysaxMultiServer Web File Access Server interface.

The login page of Sysax Multi Server Web File Access Server Interface is displayed(See Figure 16.3).

Figure 16.3. Login the Sysax Multi Server Web File Access Server Interface

The opened Sysax Multi Server Web Administration Interface is shown in Figure 16.4.

Figure 16.4. Sysax Multi Server Web Administration Interface

17

Troubleshooting Tips

This section discusses common errors and troubleshooting.

Server Cannot be Started

The selected FTP port is already being used by another program. Select another port or quit the other application.

18

How to Get Technical Support

18.1. Get technical support

Technical support for Sysax Multi Server is provided by an **online support system**. Please visit **http://www.sysax.com/support** to submit a support ticket or to check the status of an existing support ticket.

19

Frequently Asked Questions (FAQ) About Sysax Multi Server

Installation and Licensing

Does Sysax Multi Server run on Windows Vista? How about Windows 95?

Yes, Sysax Multi Server runs on all Windows operating systems from Windows 95 to Windows Vista and Windows Server 2008.

How I upgrade to a newer version of Sysax Multi Server?

You need to first uninstall the older version of the product and then install the latest version that is available on the Sysax.com website. Your server settings should not be affected by the uninstallation and reinstallation.

How do I install or update a license key?

Open the Sysax Multi Server Control panel and click the "install license" button. Select your license key file and click the "Open" button. The new license should now be installed.

How I uninstall Sysax Multi Server?

From the Windows "Start" menu, select the "Sysax Multi Server" program group and click on "Uninstall Sysax Multi Server". The uninstallation wizard will be started to complete the uninstallation of the product.

I installed the free personal edition license before my 30 day trial was up. How do I go back to the trial edition?

You can return to the trial edition within 30 days of installation by uninstalling and reinstalling the program.

What is the difference between the personal and commercial edition licenses?

The free personal edition is available for use by individuals for non commercial use. It is restricted in the number of protocols that can be simultaneously supported and the number of users that can be simultaneously logged into the server. Click here to compare all three editions side by side.

Features and Benefits

Can I run multiple protocols like FTP and SSH simultaneously?

Yes, the enterprise edition of the product can be configured to run several protocols like FTP, FTPS, SFTP, Secure Shell, Telnet, HTTP, and HTTPS simultaneously. This enables clients to connect to a user account through different mechanisms for ease of access.

Does Sysax Multi Server support secure file transfers?

Yes, the FTPS and HTTPS protocols are encrypted using SSL while the SFTP and Secure Shell protocols are encrypted with SSH based encryption.

What is HTTP and HTTPS based file transfer? Can I securely upload files using my web browser?

If the server is configured for HTTP access, clients can login to the server using any web browser and upload and download files. HTTPS provides additional security by using SSL to encrypt communication between the server and the client's web browser.

What are server event triggers and what is a server script?

An FTP script can be executed based on a connected client activity. The script can be executed when a client login is successful, client login is unsuccessful, file has been downloaded, file has been uploaded, file has been renamed, or a file has been deleted. The trigger type, user account name, client IP address, and transferred file names are automatically passed to the script. The FTP script is identical to that used by Sysax FTP Automation and supports file transfer, local file processing, email notification, external program execution, and many other actions.

Can users be authenticated using windows user accounts?

Sysax Multi Server can be configured to authenticate using windows accounts or through a custom database. It is also possible to authenticate using both mechanisms or authenticate using windows but use custom user settings.

Can I administer the program remotely using my web browser?

Yes, Sysax Multi Server can be securely administered remotely using any web browser. Using a HTTPS connection ensures that the communication is securely encrypted using SSL.

Can I make Sysax Multi Server start automatically on windows boot up?

Yes, the server can be configured to automatically start on server boot up.

Troubleshooting and Support

Why I am not able to start the server?

The most common issue is that another program is already using one or more of the ports that you selected for the server. If this is the case, the server log will contain an entry regarding this error.

How do I get technical support? How do I report a bug or request a new feature?

Please click here to use our customer support system to submit a request for technical support, report a bug or request a feature.